UNIVERSIDADE FEDERAL DE SANTA CATARINA
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

Fundamentos de Matemática Aplicada à Informática

PROF. JORGE MUNIZ BARRETO
PROF. MAURO ROISENBERG
PROFa. MARIA APARECIDA FERNANDES ALMEIDA
PROFa. KATIA COLLAZOS

FLORIANÓPOLIS, 1998

Sumário

Lista de Figuras

Lista de Tabelas

Capítulo 1

História da Matemática e da Computação

1.1 Introdução

A civilização industrial baseia-se em grande parte na ciência e na tecnologia. Entretanto, as aplicações tecnológicas com as quais nos deparamos parecem cada vez mais envolver a humanidade em um mundo "concreto", em que as imagens e comunicações reduzem dia-a-dia a necessidade de abstração, imaginação e dedução. Muitas pessoas, hoje em dia, preferem ir ao cinema ao invés de ler um livro, ou assistir ao noticiário na televisão ao invés de lê-lo no jornal ou escutá-lo no rádio.

Por outro lado, a matemática valoriza o pensamento abstrato, a formalização, a capacidade de reconhecer estruturas semelhantes sob um manto de detalhes irrelevantes. Pode-se mesmo dizer que fazer matemática não é trabalhar com números, e sim com abstrações do mundo real, envolvam ou não estas abstrações quantidades exatas e mensuráveis.

Talvez por causa disto, muitas pessoas encaram a matemática como uma disciplina afastada das conquistas e equipamentos tecnológicos, verdadeira "torre de marfim", onde se encastelam os matemáticos que passam a sua vida a pensar em coisas que não parecem ter a mínima aplicação ao mundo real em que vivemos. No entanto, isto não é verdade. A matemática é a base sobre a qual se assentam as mais importantes conquistas da ciência e da tecnologia atuais. Como o homem poderia ter chegado à Lua sem a matemática? Como estudar as estrelas? Como garantir que um computador é capaz de resolver um problema? Como a informação que chega aos nossos televisores, telefones e computadores poderia ser codificada e decodificada sem a matemática?

Com efeito, vários fatores influem na escolha dos assuntos de matemática que devem ser vistos como pré-requisitos para o desenvolvimento da Ciência da Computação. Em geral, seleciona-se os diversos tópicos da matemática que são essenciais ao estudos das diversas áreas da computação, conhecidos a grosso modo como "Matemática Discreta", deixando-se de lado os aspectos matemáticos utilizados para a modelagem de fenômenos físicos, tais com o Cálculo Diferencial e Integral, etc.

Os tópicos matemáticos que serão vistos neste trabalho são: Lógica, Teoria dos Conjuntos, Relações e Funções, Grafos, Estruturas Algébricas e Teoria Básica de Computabilidade. Apesar de procurarmos apresentar o assunto de uma maneira didática e coloquial, tentaremos manter o formalismo e a precisão adequada. Também procuraremos, sempre que possível, apresentar aplicações práticas da área da computação relacionada com os tópicos estudados.

O objetivo principal deste capítulo é tentar situar a matemática através de uma rápida visão panorâmica da história da matemática, ressaltando os elementos históricos relacionados com a própria história da computação. Não é por acaso que muitos cientistas, responsáveis por grandes feitos e impulsos no desenvolvimento dos computadores e da computação em geral, como Pascal, Babbage, Von Neumann e Turing, entre outros, eram matemáticos.

1.2 As Origens

As origens da matemática remontam ao próprio início da história da humanidade. Os primeiros passos do pensamento matemático provavelmente estavam associados ao ato de contar coleções de objetos discretos, e os dedos das mãos poderiam ser utilizados para indicar conjuntos de um, dois, três, quatro ou cinco objetos, tais como um lobo, duas árvores, três ovelhas e assim por diante.

A descoberta da escrita deu um grande impulso nas habilidades matemáticas, assim como permitiu que através da arqueologia pudessemos conhecer como a matemática evoluiu nos quatro milênios que antecederam a era cristã.

Foi o desenvolvimento da agricultura que tornou o homem sedentário e possibilitou o aparecimento das grandes civilizações surgidas na Mesopotâmia (os babilônios) e nas margens do Rio Nilo (os egípcios). Este desenvolvimento agrícola só foi possível graças a utilização de um calendário e de sistemas de irrigação.

O desenvolvimento de um calendário pressupõe algum desenvolvimento da aritmética, de técnicas de observação astronômica e de sistemas de medição de ângulos. Entre o IV e o III Milênios AC desenvolveram-se sistemas de calendário bastante apura-

41	59
1	59
2	118
4	236
8	472
16	944
32	1888

Tabela 1.1: Tabela para multiplicar 41 por 59 pelo método egípcio

dos na Mesopotâmia e no Egito que já permitiam prever com razoável precisão as épocas de enchente, plantio e colheita. Também os sistemas de irrigação exigiam conhecimentos primitivos de engenharia e agrimensura. Com a agricultura abundante, floresceu o comércio e a troca de mercadorias, o que exigia conhecimentos de aritmética aplicada.

Os babilônios, que sucederam os sumérios na Mesopotâmia no final do terceiro milênio AC possuiam um avançado sistema de numeração. Este era um sistema posicional com base 60 (o nosso sistema de numeração atual é em base 10). Eles dividiam o dia em 24 horas, cada hora em 60 minutos e cada minuto em 60 segundo. Talvez o aspecto mais interessante das habilidades de cálculo dos babilônios sejam as suas tabelas para auxílio ao cálculo.

Para tornar a multiplicação mais fácil, os babilônios usavam a fórmula $a.b = ((a+b)^2 - a^2 - b^2)/2$, sendo esta a razão da existência das tabelas de quadrados de números, achadas por arqueólogos.

Os egípcios, assim como os romanos possuiam um sistema de numeração que não era muito adequado para operações aritméticas. No entanto, os egípcios eram muito pragmáticos em sua utilização da matemática. Em um papiro datado de 1850 AC, encontra-se um exemplo numérico concreto do cálculo do volume de um tronco de pirâmide de base quadrada. Em outro papiro, chamado de papiro de Rhind, encontra-se a recomendação de como multiplicar 41 por 59. "Pegue 59 e some a ele mesmo, então some o resultado com ele mesmo e assim por diante".

Como 64 é maior que 41, não é necessário continuar. proceda-se agora as seguintes subtrações:

$$41 - 32 = 9, 9 - 8 = 1, 1 - 1 = 0$$

Agora selecione os números da coluna da direita correspondentes aos fatores 32, 8 e 1 e some-os:

$$1888 + 472 + 1 = 2419$$

Note-se que a multiplicação é obtida utlizando-se apenas operações de adição.

Outro fator impulsionador do desenvolvimento da matemática, além da agricultura e do comércio, estão os rituais religiosos e funerários. Tome como exemplo as próprias pirâmides do Egito e os grandes monumentos de pedra (megalitos) espalhados pela Europa e Norte da África. Acredita-se que Stonehenge, na Inglaterra, foi construído entre 1900 e 1600 AC e muitos historiadores afirmam que ele era utilizado como uma "calculadora de pedra" com o objetivo de prever o nascimento do Sol e da Lua no solstício e no equinócio.

1.3 A Matemática na Grécia

Provavelmente o contato dos gregos com o Império Persa durante o século VI AC trouxe aos gregos consideráveis conhecimentos dos antigos povos do Oriente Médio. A revolução do pensamento metemátic o na Grécia começou devido a um forte espírito do curiosidade, de atividades racionalistas e da crença de que o homem poderia entender o mundo e a si próprio. Através de Thales e Pitágoras, ainda no século VI AC, o pensamento matemático grego começou a adquirir características familiares aos matemáticos contemporâneos: 1) necessidade de definições precisas; 2) preocupação com explicitar pressuposições; 3) desenvolvimento do pensamento dedutivo e seu emprego para unificar o pensamento matemático da época; 4) noção de pesquisa, formulação clara dos problemas e distinção nítida entre uma conjectura e um teorema demonstrado.

Na Grécia a filosofia e a matemática estavam intimamente relacionadas e várias discussões e análises críticas foram surgindo. Os processos infinitos (de limite) que se usava na geometria sofreram uma profunda análise crítica nos trabalhos de Zeno de Elea.

É da Grécia também o berço do raciocínio lógico e da Lógica como disciplina matemática. No início, Lógica era expressa em linguagem natural pelos filósofos de Atenas. Raciocínios tipicamente lógicos se encontram em diálogos de Sócrates com seus discípulos e depois em Platão. Mas foi com Aristóteles que a Lógica tomou um caráter independente de outras formas de pensamento.

Com a primeira escola de matemática de Alexandria, fundada no fim do século IV

AC, surge a monumental obra de Euclides (365-275 AC) "Elementos" (Stoichia), que incorporava o trabalho de seus predecessores e suas próprias contribuições, expondo a geometria do plano e do espaço de forma dedutiva.

A matemática grega chegaria ao seu apogeu com Arquimedes (287-212 AC). Sua contribuição à geometria é rigoraso e cheia de imaginação. Não menos engenhosas foram suas contribuições para o estudo da mecânica e da hidrostática.

A partir do século II AC ocorre o declínio geral do progresso matemático. Até a queda do Império Romano, a atividade matemática praticamente desapareceu do mundo ocidental. O crepúsculo da civilização do Mundo Antigo atinge assim, também a matemática. Como legado, os gregos nos deixaram grandes conhecimentos sobre a lógica, os números e as formas geométricas. Eles também nos legaram a inspiração de que a Natureza seria passível de ser conhecida e explicada pela razão, utilizando-se como instrumento racional a matemática.

1.4 Os Tempos de Escuridão

Enquanto na Idade Média o pensamento matemático passava por um período de escuridão intelectual, a matemática se desenvolvia nos centros de cultura do Mundo Árabe, onde os textos matemáticos gregos foram preservados e traduzidos. A matemática árabe se concentrava particularmente nas áreas de álgebra e trigonometria. Deste trabalho podemos destacar os trabalhos de Al-Khowarismi e de Bhaskara. Vêm dos árabes e dos hindus o aperfeiçoamento do sistema posicional decimal, incluindo a representação do número zero.

1.5 O Renascimento

A agitação artstica, intelectual e cultural durante a Renascença (séculos XVI, XVII e XVIII) atinge a filosofia, a ciência e a matemática. Nesta época, a obra de Arquimedes é traduzida para o latim. As atividades científicas e matemáticas são estimuladas por problemas práticos, como a construção de canais, moinhos d'água, construção naval, cartografia e navegações. O aprimoramento tecnológico e a curiosidade científica caminhavam juntas. O interesse pela mecânica teórica levou ao desenvolvimento do cálculo diferencial e integral como ferramenta para modelar e explicar os fenômenos físicos.

Um grande progresso matemático é alcançado nesta época. Fermat e Descartes desenvolvem a geometria analítica; Newton e Leibnitz, o cálculo diferencial e inte-

gral; Fermat e Pascal iniciam a teoria da probabilidade; Galileo e Newton aplicam a matemática para fundamentar a dinâmica, resultando no Teoria da Gravidade de Newton. Com apenas dezoito anos, Pascal direcionou seus interesses para o projeto e construção de uma máquina calculadora. Em poucos anos, por volta de cinquenta destas máquinas haviam sido vendidas.

Muitas das características do mundo moderno têm suas origens na efervescência deste período. A partir de então a matemática estava firmemente estabelecida como base de todo o desenvolvimento científico.

1.6 Os Tempos Modernos

No final do século XVIII e no início do século XIX, o período de entusiasmo criador dos dois séculos anteriores diminui gradualmente. Se antes a matemática se apoiava em inspiração e intuição, não se preocupando muito com o formalismo e o rigor, agora, se procura bases rigorosas para apoiar o crescimento de pesquisas puras e aplicadas.

O primeiro grande vulto deste período é Carl-Friedrich Gauss (1775-1855). Suas contribuições abrangem toda a matemática de época: álgebra, aritmética, análise, geometria diferencial, geometria não-euclidiana, funções analíticas, mecânica celeste, etc. H. N. Abel (1802-1829) procura fundamente a teoria da convergência de séries numéricas e de séries de funções; A. L. Cauchy (1789-1857) se ocupa de formalizar a teoria dos limites e da integral definida.

Em 1833, Charles Babbage (1791-1871) concebeu uma máquina considerada por muitos como a antecessora dos modernos computadores, por trazer a idéia de "programa" armazenado, sendo o primeiro programa a ser escrito feito por uma de suas amigas, Lady Lovelace cujo primeiro nome serviu para designar uma linguagem de programação, *Ada*. Inicialmente ele construiu a máquina chamada "Difference Engine" [11]. Seu sucesso o fez conceber uma outra, bem mais complexa que denominou "Analytical Engine" e que não chegou a completar e que se tivesse sido concluída, realizaria todas as operações aritméticas e armazenaria informações para utilização posterior. Isto seria feito através de um complexo mecanismo de rodas, engrenagens e alavancas. A máquina nunca foi concluída devido ao corte de verbas. Babbage pode ser considerado, com sua invenção, um precursor das idéias interdisciplinares. Com efeito, em sua época, dava-se enorme importância ao que se chamavam *autômatos* e que iam desde bonecos que se mexiam até complicados relógios mecânicos, tais como o da catedral de Estrasburgo, na França, fronteira com

a Alemanha. Além disto, Babbage costumava freqüentar reuniões femininas, onde muitas mulheres se dedicavam ao trabalho com teares. Ora, os teares utilizavam fitas perfuradas, a posição dos furos comandando o ponto a ser feito. Unindo as duas idéias, autômatos e teares nasceu a "Máquina Analítica", ou em suas próprias palavras :"*The calculating part of the engine may be divided into two portions: 1st, the mill in which all operations are performed; 2nd, the store in which all numbers are originally placed and to which the numbers computed by the engine are returned.* (C.Babbage, 26 Dec. 1837 in Randel, página75 [**?**])". Foi com ele que nasceu a noção de CPU e memórias separados.

Na área de fundamentos matemáticos, uma teoria logicamente satisfatória dos números reais só veio a aparecer na segunda metade do século XIX, com os trabalhos de Dedekind (1831-1916), Weirstrass (1815-1897) e Georg Cantor (1845-1918). Estes matemáticos procuraram mostrar como construir uma teoria satisfatória dos número reais $\Re$. Além da análise lógica dos reais, no fim do século XIX, a análise axiomática de Guiuseppe Peano (1858-1932) procurou situar logicamente os números naturais. Também se procurou a construção dos inteiros naturais por meio de uma lógica de classes, primeiramente através de Frege (1848-1925) e, posteriormente e de maneira independente por Bertrand Russel e Whitehead nos *Pricipia Mathematica*A idéia da lógica matemática como instrumento de análise floresce a partir deste período.

Os estudos de Cantor procurando explicar logicamente os números reais foram seguidos por suas pesquisas pioneiras na teoria dos conjutos e dos números transfinitos Mais tarde, a teoria dos conjutos, aperfeiçoada no século XX por Zermelo e Frenkel entre outros, foi reconhecida como o principal ponto de partida para a construção dos demais ramos da matemática (álgebra, topologia, etc). O método axiomático, usado no século XIX no estudo das geometrias não-euclidianas e da geometria projetiva, foi gradualmente fortalecido pelos trabalhos de Hilbert. David Hilbert se notabilizou por promover a abordagem axiomática da matemática; pelos trabalhos no espaço dimensional infinito, mais tarde chamado de "Espaço de Hilbert"; e principalmente pelos 23 problemas propostos no segundo Congresso Internacional de Matemática de Paris. Estes problemas desafiaram, e ainda hoje desafiam, os matemáticos a solucionar questões fundamentais.

De certa maneira, os formalismos matemáticos dos axiomas defendidos por Hilbert foram enfraquecidos por Karl Gödel (1906-1978). Gödel se tornou conhecido ao provar que em qualquer sistema matemático axiomático consistente existirão proposições que não podem ser provadas verdadeiras ou falsas. Por outro lado, se todos as proposições foram ou verdadeiras ou falsas conclui-se que os axiomas são inconsistentes. Os resultados de Gödel mostraram que a matemática não é um objeto

acabado, o que significa que um computador nunca poderá ser programado para responder todas as questões matemáticas.

1.7 A Era dos Computadores

Pode se dizer que a era moderna da computação começou com implementações mecânicas, quase simultaneamente em vários países. O pioneirismo nas máquinas eletromecânicas cabe a H. Hollerith (1860-1929) que construiu, para ajudar o censo demográfico dos Estados Unidos de 1890, o ancestral comum destas máquinas.

Foi com este tipo de máquina que se fez a primeira aplicação em escritórios. D. E. Felt e W. Burroughs (1857-1898) depois de lançar o "Comptometer" (1885), que era muito difícil de utilizar, lançaram a "L'ADDING AND LISTING MACHINE" primeira máquina trabalhando sobre o conceito de lista como se conhece hoje.

Nos Estados Unidos, por volta de 1925 no Massachusetts Institute of Technology (MIT), Vannevar Bush e seus colegas iniciaram a construção de um grande analisador diferencial [1] financiado pela "Rockefeller Foundation" e que foi concuido em 1930. Em 1939, a IBM iniciou a construção do MARK I, um equipamento eletro-mecânico completamente automático, e que seguia os princípios propostos por Babbage. Antes que o MARK I pudesse ser completado, em 1944 ele foi suplantado pelo projeto do ENIAC (Electronic Numerical Integrator and Calculator), a primeira calculadora totalmente eletrônica. Neste projeto participava John Von Neuman, que entre 44 e 46 elaborou relatórios para o exército sobre as capacidades computacionais do equipamento. Em 1949, o primeiro computador americano, que muitos acreditam ser o primeiro no mundo com programa armazenado, entrou em operação. Dois anos depois, o UNIVAC I (Universal Automatic Calculator) foi terminado pela Sperry Rand Corporation.

Enquanto muitos enxergavam no computador apenas uma poderosa e veloz máquina de calcular, em 1945 Alan Turing escreveu o seu conceito de computador, uma máquina universal, não necessariamente ligada a idéias de uma calculadora, mas sim, a manipulação lógica de símbolos. Turing foi um dos responsáveis pela estrutura de programa e de linguagens.

Na França pode-se citar o trabalho pioneiro de Louis Coufignal cuja tese de doutorado apresentava em 1938, máquina de calcular capaz de realizar cálculos tão variados quanto os da macânica celeste [3].

Na então União Soviética [4] apenas em 1947 S. A. Lebadev iniciou a construção,

[1] Computador capaz de resolver um sistema de equações diferenciais.

em Kiev do calculador MESM concluido em 1950. Dele descendem o BESM e o STRELA concluídos em 1953. Nesta época já havia começado a aparecer os MINSK, da Universidade de Moscow, computadores especializados dos quais mais de 2000 foram construídos até 1976.

Finalmente cabe mencionar o trabalho pioneiro de Zuse e Schreyer na Alemanha. O trabalho destes dois pioneiros sś foi conhecido fora da Alemanha depois do final da II Guerrra Mundial (1945) e ainda hoje é desconhecido de muitos. Konrad Zuse (1910-) iniciou a construção de sua calculadora em 1934 quando era estudante da "Technische Hochsch Berlin-Charlottenburg". Em 1936 ele havia construído uma calculadora dotada de uma unidade aritmética usando o conceito de ponto flutuante ([11], cap'ıtulo IV), primeira no mundo. Baseando-se nas idéias de Babbage, Leibnitz, Torres y Quevedo e Ludgate ele foi o pioneiro em máquina programável. Seu pedido de patente do *Z1* data de 11/04/1936 ([11] p.159). Não existem registros de quando o então "Diploma Engineer" iniciou seu doutorado auxiliado pelo jóvem Helmut Theodore Schreyer. Schreyer projetou e construiu um protótipo de válvula duplo-triodo, fabricada depois pela Telefunken, para ser usada em nova versão do computador patenteado por Zuse, desta vez eletrônico. O que é certo é que em 1939, Zuse foi convocado para o serviço militar e Schreyer escreveu um relatório apresentado ao exército alemão, mostrando a importância dos computadores. Para mostrar a importância do uso de válvulas e a velocidade de cálculo que seria atingida ele escreve: "Ele pode também ser útil para calcular tabelas de tiro de artilharia e para o cálculo da trajetória de foguetes de longo alcance, pois pode instantaneamente produzir dados para o posicionamento do canhão se as informaçõers necessárias são introduzidas na máquina" ([11] p.169).

Apesar de não terem conseguido subsídio para a construção da máquina que desejavam, com 1500 válvulas, Zuse foi dispensado do serviço militar. Não restou nenhuma destas máquinas após a guerra, a última, o *Z4*, tendo sido destruída dentro de um vagão de trem por um bombardeio perto do final da guerra. Schreyer que viajava no trem conseguiu escapar e, chegando a Embaixada do Brasil em Viena, conseguiu um passaporte de "brasileiro nato!". E foi assim que ele chegou ao Rio de Janeiro (sem falar uma palavra de português) no final de 1945. Conseguiu um lugar como professor de Telefonia na então Escola Técnica do Exército, hoje, Instituto Militar de Engenharia.

Neste Instituto conseguiu, em 1958, depois de mais de 10 anos de tentativas, convencer as autoridades acadêmicas de construir com auxílio de projetos de fim do curso de eletrônica, um computador. Foi assim que as turmas de 1958,1959 e 1960, trabalharam neste projeto, usando muitos componentes de sucata de guerra obtidos

no Depósito de Material de Comunicações no Rio de Janeiro (radares, radios, etc.) finalizado o computador em 06 de janeiro de 1961, data da formatura da última turma [2] da ainda Escola Técnica do Exército.

Schreyer nasceu alemão. Construiu o primeiro computador totalmente eletrônico. Veio para o Brasil, onde não acrecditaram no que contou, mas conseguiu orientar alunos, construindo o primeiro computador (era híbrido, parte analógica e parte digital) eletrônico no Brasil [2] concluído em 1960 e desmontado no desmenbramento da Escola Técnica do Exército (ETE) em Instituto Militar de Engenharia(IME) e Instituto de Pesquisa e Desenvolvimento (IPD), provavelmente para evitar a remoção para o IPD. Morreu brasileiro, em seu apartamento no Flamengo, tendo construído o primeiro computador digital eletrônico programável com válvulas, que ele mesmo projetou antes da guerra, e tendo coordenado o projeto do primeiro computador projetado e construído no Brasil.

Hoje em dia os computadores se tornaram tão rápidos e poderosos que ultrapassaram em muito os sonhos de desejos de Babbage, que viveu apenas um século antes do seu surgimento. problemas que estavam, até bem pouco tempo, muito além das capacidades dos matemáticos, hoje em dia têm sido solucionados com o auxílio dos computadores.

Capítulo 2

Lógica

Como em muitos outros campos de estudo é difícil dar uma definição precisa de Lógica. A Encyclopaedia Britannica (edição 1957) diz: *"Logic is the systematic study of the structure of propositions and of the general conditions of valid inference by a method which abstracts from the content or matter of the propositions and deals only with their logical form".* Apesar de ser uma definição recursiva por definir lógica em função do termo forma lógica, esta definição ressalta dois pontos característicos da Lógica contemporânea: o estudo dos mecanismos *válidos* de inferência e a importância da forma da apresentação. O primeiro destes pontos, mecanismos *válidos* subentende a dualidade de valores de verdade e o segundo ponto leva ao termo *Lógica Formal.* Aqui se considera a definição acima, modificada apenas pela omissão da palavra *válidos.* Desta forma, sendo a Lógica o estudo dos mecanismos do pensamento é natural que a Lógica ocupe um papel de destaque na área da Computação conhecida como em Inteligência Artificial, tanto na representação do conhecimento como paradigma na resolução de problemas.

Neste capítulo se apresenta uma introdução à Lógica, começando por um histórico sobre a sua evolução, e aprofundando-se o estudo da Lógica de Primeira Ordem, especialmente o Cálculo Proposicional e o Cálculo de Predicados.

2.1 Notas Históricas

Os primeiros princípios referentes à Lógica podem ser atribuídos ao grego Aristóteles. A maioria das contribuições de Aristóteles para a Lógica se encontram em um grupo de livros conhecidos por *Organon.* O *Organon* compreende várias partes: *Categorias*, *As Interpretações*, *Analítica*, *Tópicos*, e o *Refutações Sofísticas.* Todos os textos estão no estilo característico de Aristóteles, ou seja tipo caderno de notas abreviadas.

O núcleo do pensamento Aristotélico se encontra nos primeiros sete capítulos do primeiro volume do *Analítica*, ou *Primeiro Analítica*. É aí que ele apresenta a teoria dos *silogismos*, descoberta intelectual de inigualável amplitude e que dominou a Lógica por mais de 2000 anos, e ainda hoje prevalece na cultura científica.

A definição aristotélica de silogismo é: "*silogismo é uma frase na qual, tendo se afirmado algumas coisas, algo além destas coisas se tornam verdadeiras.*"

Base da Lógica Contemporânea, os silogismos enunciados por Aristóteles são muitas vezes mencionados, utilzados, deturpados e poucas vezes compreendidos. Note-se que em todo o trabalho de Aristóteles não existe menção a objetos particulares, o que significa que o exemplo clássico de silogismo abaixo, não é aristotélico:

"Todos os homens são mortais

Sócrates é um homem

Então, Sócrates é mortal."

A lógica aristotélica pode ser considerada lógica formal no sentido de que ela se ocupa apenas da forma do pensamento, sem levar em consideração os objetos particulares em que se pensa. Além disso, ela estabelece o modo de fazer inferências válidas. Note-se que não se deve confundir os termos formal e formalismo, este último significando uma linguagem precisa utilizada para escrever raciocínios formais.

Nos séculos que se seguiram, a filosofia floresceu na Grécia, servindo de alimento à curiosidade intelectual daqueles que eram motivados por valores culturais. Sob vários aspectos, os lógicos atingiram o seu zenite com os Estoícos e os Megarianos. A escola megariana foi fundada por Euclides que teve como discípulo Eubulides, a quem se atribue o **paradoxo do mentiroso**. Este paradoxo é apresentado sob várias formas, sendo talvez a mais comum a de Cícero: *"Se você diz que está mentindo e está dizendo a verdade então você está mentindo?"*.

Zeno foi formado nesta escola e foi o fundador do Estoicismo. Um exemplo de argumento estóico é:

"Se você sabe que está morto, você está morto,

Mas se você sabe que está morto, você não está morto,

portanto você não sabe se está morto ou não."

Mas talvez o mais famoso seja: **o paradoxo do barbeiro**

"Havia uma pequena cidade onde só existia um barbeiro. O barbeiro recebeu a missão de barbear todos os homens que não barbeavam a si mesmos. Se não o fizesse morreria!"

Pergunta: Quem barbeia o barbeiro?

O paradoxo resume-se no fato de que, se ele se barbeasse, estaria barbeando uma

pessoa que barbeia a si mesmo e se não o fizesse, estaria deixando de barbear alguém que não se barbeia.

Estes argumentos alimentaram profunda especulação intelectual para filósofos desde então, principalmente na Grécia antiga, os quais notaram ser o axioma do *meio excluído* o ponto crucial. Este axioma considera que as proposições podem ter apenas dois valores de verdade, verdadeiras ou falsas. Valores intermediários de verdade sendo excluídos.

A Lógica contemporânea se caracteriza por dois pontos?

- Pela tendência chamada *matematização da lógica*, movimento que pode ser atribuído à Frege e Russel que invadiu a Lógica de um extensivo uso de símbolos e pelo desejo de dar uma base sólida a conceitos matemáticos.

- O reconhecimento das *Lógicas Não-Padrão*. A Lógica baseada nos trabalhos de George Boole usando dois valores de verdade sendo conhecida como *Lógica Padrão* e compreendendo o Cálculo das Proposições e o Cálculo dos Predicados, ambos constituindo a *Lógica de Primeira Ordem*. As Lógicas Não-Padrão compreendendo as Lógicas de Ordem Superior,

Extensões não monotônicas são aquelas em que alguns teoremas da Lógica padrão deixam de ser válidos. Talvez o mais notável exemplo seja o clássico postulado do *meio excluido* que deixa de ser válido nas Lógicas multi-valoradas das quais Lukasiewicz foi pioneiro.

2.2 Lógica de Primeira Ordem

A Lógica de Primeira Ordem compreende o *Cálculo das Proposições* e o *Cálculo dos Predicados*. Informalmente, o *Cálculo das Proposições* envolve apenas constantes e o *Cálculo dos Predicados* considera ainda variáveis e quantificadores sobre estas variáveis (ex: Para todo x; Existe x). Entretanto uma sentença não pode ser quantificada pois se estaria tratando de Lógica de Segunda Ordem. Por exemplo, a sentença "para todas as sentenças..." pertence à Lógica de Segunda Ordem.

2.3 Cálculo Proposicional

O Cálculo Proposicional se interessa pelas sentenças declarativas, as proposições, que podem ser verdadeiras ou falsas. O Cálculo das Proposições compreende a sua

sintaxe e a sua semântica. Sua principal finalidade é a de dada uma proposição com sintaxe correta e a semântica dos componentes da proposição, determinar o valor semântico da proposição.

Exemplos de Proposições:

1. Hoje é segunda ou terça-feira
   Hoje não é terça-feira
   $\vdash$ Hoje é segunda.

2. Rembrandt pintou a Mona Lisa ou Michelângelo à pintou
   Não foi Rembrandt que pintou a Mona Lisa
   $\vdash$ Michelângelo pintou a Mona Lisa

3. $p \vee q \Leftarrow$ p ou q
   $\neg p \Leftarrow$ não é o caso que p
   $\vdash q \Leftarrow$ q

2.3.1 Sintaxe do Cálculo Proposicional

A sintaxe do Cálculo das Proposições especifica os símbolos e os modos de combiná-los para formar uma expressão válida da linguagem, as quais costumam ser chamadas *fórmulas bem formadas* (fbf) (do inglês "Well Formed Formulas" - wff).

Elementos Válidos da Linguagem

- Conectivos ou Operadores Lógicos
  - Negação: não é o caso que $(\neg)(\sim)$
  - Conjunção: e $(\&)(\wedge)$
  - Disjunção: ou $(\vee)$
  - Condicional: se ... então $(\rightarrow)(\Rightarrow)$
  - Bicondicional: se e somente se $(\leftrightarrow)(\Leftrightarrow)$
- Letras Sentenciais
  - Letras maiúsculas seguidas ou não de números
- Parênteses
  - (,)

Fórmulas Atômicas

No Cálculo Proposicional, são os símbolos que representam as sentenças declarativas, no caso, as letras sentenciais.

Fórmula Bem Formada

- Uma fórmula atômica é uma fórmula bem formada (fbf);
- Uma fbf precedida por $\neg$ é uma fbf;
- Uma fórmula atômica seguida por um conetivo distinto de $\neg$ e uma fbf, é uma fbf.

Ex.: Se não está chovendo, então não é o caso que está chovendo e nevando. $\neg C \rightarrow \neg(C \wedge N)$

2.3.2 Semântica do Cálculo Proposicional

Uma fbf pode ter uma interpretação a qual define a semântica da linguagem. Uma interpretação pode ser considerada como um mapeamento do conjunto das fbfs para um conjunto de valores de verdade que na lógica dicotômica é o conjunto $\{Verdadeiro, Falso\}$ ou $\{V, F\}$.

A semântica dos conectivos mais conhecidos é:

- $A \wedge B$ é verdade se A é verdade e B é verdade;
- $A \vee B$ é verdade se qualquer dos dois, A ou B é verdade;
- $A \rightarrow B$ significa que se A é verdade, B é verdade. Entretanto nada se sabe de B se A for falso.

2.3.3 Tabelas-Verdade

As Tabelas-Verdade fornecem um teste rigoroso e completo para a validade ou invalidade de formas de argumento da Lógica Proposicional, além de se constituir em um algoritmo. Quando existe um algoritmo que determina se as formas de argumento expressáveis num sistema formal são válidos ou não, esse sistema é dito decidível. Desta forma, eles garantem a decidibilidade da Lógica Proposicional.

O Condicional normalmente parece um conceito bastante confuso para o iniciante, principalmente quando se tenta converter um condicional expresso em Português para uma forma simbólica.

Negação	
A	$\neg A$
V	F
F	V

Tabela 2.1: Tabela-Verdade para o operador de Negação

Conjunção		
A	B	$A \wedge B$
V	V	V
V	F	F
F	V	F
F	F	F

Tabela 2.2: Tabela-Verdade para a Conjunção

Disjunção		
A	B	$A \vee B$
V	V	V
V	F	V
F	V	V
F	F	F

Tabela 2.3: Tabela-Verdade para a Disjunção

Condicional		
A	B	$A \rightarrow B$
V	V	V
V	F	F
F	V	V
F	F	V

Tabela 2.4: Tabela-Verdade para o Condiconal

Bicondicional		
A	B	$A \leftrightarrow B$
V	V	V
V	F	F
F	V	F
F	F	V

Tabela 2.5: Tabela-Verdade para o Bicondiconal

Geralmente assumimos uma relação, ou implicação ou sentimento de causa-e-efeito entre o antecedente e o consequente de um condicional. Por exemplo, a sentença: *Se eu pegar o livro, então deverei lê-lo esta noite*, parece razoável porque o consequente se refere ao livro mencionado na primeira parte da senteça. Por outro lado, a sentença: *Se eu pegar o livro, então a sala é vermelha*, parece não fazer sentido. Entretanto, de acordo com a definição de condicional, esta última sentença é perfeitamente aceitável e possui um valor de verdade que vai depender dos valores de verdade das senteças declarativas que estão sendo conectadas.

Se A e B são quaisquer duas senteças declarativas, então a proposição $A \leftrightarrow B$, que é lida como: *"A se e somente se B"*, é chamada de Bicondicional. Note que os valores de verdade de $(A \rightarrow B) \wedge (B \rightarrow A)$ são idênticos aos valores de verdade de $A \leftrightarrow B$ aqui definidos.

2.3.4 Tautologia

Proposição que é sempre verdade, independentemente dos valores de seus componentes.

Ex.: $A \vee \neg A$

A	$\neg A$	$A \vee \neg A$
V	F	V
F	V	V

2.3.5 Fórmula Inconsistente ou Contradição

Proposição que é sempre falsa para todas as suas interpretações.

Ex.: $A \wedge \neg A$

A	$\neg A$	$A \wedge \neg A$
V	F	F
F	V	F

2.3.6 Equivalência de Fórmulas

Sejam A e B duas fbfs e sejam $P_1, P_2, ..., P_n$ as letras sentencias que ocorrem em A e em B. Se os valores de verdade de A forem iguais aos valores de verdade de B para todos os 2^n possíveis valores de verdade atribuídos a $P_1, P_2, ..., P_n$, então A e B são ditos equivalentes.

Abaixo aparecem alguns exemplos de fórmulas que são equivalentes e cujas equivalências podem ser verificadas através de tabelas-verdade.

$\neg\neg A = A$

$A \vee A = A$

$(A \wedge \neg A) \vee B = B$

$A \vee \neg A = B \vee \neg B$

Exemplos:

Prove que:

$P \rightarrow Q = \neg P \vee Q$

$P \rightarrow Q = \neg(P \wedge \neg Q)$

P	Q	$\neg P$	$\neg P \vee Q$	$P \rightarrow Q$	$\neg Q$	$P \wedge \neg Q$	$\neg(P \wedge \neg Q)$
V	V	F	V	V	F	F	V
V	F	F	F	F	V	V	F
F	V	V	V	V	F	F	V
F	F	V	V	V	V	F	V

Uma tabela de equivalência de fórmulas também pode ser utilizada para provar a equivalência entre duas fórmulas sem que seja necessária a construção da tabela-verdade.

Exemplo:

Mostre que

$(\neg P \wedge (\neg Q \wedge R)) \vee (Q \wedge R) \vee (P \wedge R) = R$

$(\neg P \wedge (\neg Q \wedge R)) \vee (Q \wedge R) \vee (P \wedge R) =$

$(\neg P \wedge (\neg Q \wedge R)) \vee (R \wedge (Q \vee P) =$ (Distr.)

$((\neg P \wedge \neg Q) \wedge R) \vee (R \wedge (Q \vee P) =$ (Comut.)

$((\neg P \wedge \neg Q) \vee (Q \vee P)) \wedge R =$ (Distr.)

$(\neg(P \vee Q) \vee (P \vee Q)) \wedge R =$ (De Morgan e Comut.)

$(\neg A \vee A) \wedge R =$

$Tautologia \wedge R = R$

EQUIVALÊNCIA	NOME
$\neg(A \wedge B) = (\neg A \vee \neg B)$	Lei de De Morgan
$\neg(A \vee B) = (\neg A \wedge \neg B)$	Lei de De Morgan
$A \wedge B = B \wedge A$	Comutatividade
$A \vee B = B \vee A$	Comutatividade
$A \vee (B \vee C) = (A \vee B) \vee C$	Associatividade
$A \wedge (B \wedge C) = (A \wedge B) \wedge C$	Associatividade
$A \wedge (B \vee C) = (A \wedge B) \vee (A \wedge C)$	Distributividade
$A \vee (B \wedge C) = (A \vee B) \wedge (A \vee C)$	Distributividade
$A = \neg(\neg A)$	Dupla Negação
$A \rightarrow B = \neg B \rightarrow \neg A$	Transposição
$(A \wedge B) \rightarrow C = A \rightarrow (B \rightarrow C)$	Exportação
$A \wedge A = A$	Idempotência
$A \vee A = A$	Idempotência

Tabela 2.6: Tabela de equivalências de fórmulas

As regras de equivalencia também podem ser utilizadas para simplificação de fórmulas, permitindo escrever fórmulas equivalentes mais simples e compactas, eliminado letras sentenciais supérfluas.

Exemplo:
Simplifique a seguinte fbf: $A \vee (A \wedge (\neg A \wedge B \vee C \wedge (A \wedge C)))$
$A \vee (A \wedge (\neg A \wedge B \vee A \wedge C))$ (Assoc. e Idemp.)
$A \vee (A \wedge (\neg A \wedge B) \vee A \wedge (A \wedge C))$ (Distr.)
$A \vee ((A \wedge \neg A) \wedge B) \vee A \wedge C)$ (Assoc.e Idemp.)
$A \vee (Falso \wedge B) \vee A \wedge C)$ (Contrad.)
$A \vee (Falso \vee A \wedge C)$
$A \vee (A \wedge C)$
$(A \vee A) \wedge (A \vee C)$
A

2.3.7 Regras de Inferência

Regras de Inferência são regras de reescrita que permitem produzir novas fbfs a partir de outras. Seu uso pode ser visto como uma forma de provar teoremas, onde as novas fórmulas são teoremas provados. Através das regras de inferência podemos

demonstrar que uma dada fórmula é uma conseqüência válida de um dado conjunto de premissas. As regras de inferência são basicamente os silogismos de Aristóteles, formulados de modo mais atual.

Regras Básicas

1. Modus Ponens (MP): De um condicional e seu antecedente podemos inferir a seu conseqüente. $A, A \to B \vdash B$.

   Exemplos:

   - Se aquele animal for um gato, então aquele animal é preguiçoso.
     Aquele animal é um gato.
     Logo, aquele animal é preguiçoso.
   - Se Maria ou Juliana vier, então a festa será alegre e divertida.
     Maria ou Juliana virão.
     Logo, a festa será alegre e divertida.

   Ex.: $P, P \to Q, Q \to R \vdash R$ [1]

   Prova:

1	P	P
2	$P \to Q$	P
3	$Q \to R$	P
4	Q	$1, 2MP$
5	R	$3, 4MP$

2. Eliminação da Negação ($\neg E$): De uma fbf $\neg\neg A$, podemos inferir A.

   Exemplo:

   - Não é o caso de que o lixo não está vazio.
     Logo, o lixo está vazio.

   Ex.: $\neg P \to \neg\neg Q, \neg\neg\neg P \vdash Q$

[1] O símbolo $\vdash$, chamado "traço de asserção", afirma que a fórmula à sua direita pode ser deduzida utilizando como premissas somente as fórmulas que estão à sua esquerda.

Prova:

1	$\neg P \rightarrow \neg\neg Q$	P
2	$\neg\neg\neg P$	P
3	$\neg P$	$2\neg E$
4	$\neg\neg Q$	$3, 1 MP$
5	Q	$4\neg E$

3. Introdução da Conjunção ($\wedge I$): De quaisquer fbfs A e B, podemos inferir $A \wedge B$.

4. Eliminação da Conjunção ($\wedge E$): De uma conjunção podemos inferir qualquer uma de suas sentenças.

   - A sala está vazia.

     O professor está dando aula.

     Logo, a sala está vazia E o professor está dando aula.

   - João E Marcelo jogarão futebol este sábado.

     Logo, João jogará futebol este sábado.

   Ex.: $P \rightarrow (Q \wedge R), P \vdash P \wedge Q$

   Prova:

1	$P \rightarrow (Q \wedge R)$	P
2	P	P
3	$Q \wedge R$	$2, 1 MP$
4	Q	$3 \wedge E$
5	$P \wedge Q$	$2, 4 \wedge I$

5. Introdução da Disjunção ($\vee I$): De uma fbf A, podemos inferir a disjunção de A com qualquer fbf.

   Exemplo:

   - A sala está vazia.

     Logo, a sala está vazia OU o professor está dando aula.

   Ex.: $P \vdash (P \vee Q) \wedge (P \vee R)$

Prova:

1	P	P
2	$P \vee Q$	$1 \vee I$
3	$Q \vee Q$	$1 \vee I$
4	$(P \vee Q) \wedge (P \vee R)$	$2,3 \wedge I$

6. Eliminação da Disjunção ($\vee E$): De fbfs da forma $A \vee B$, $A \rightarrow C$ e $B \rightarrow C$, podemos inferir C.

   Exemplo:

   - Eu OU meu irmão ficaremos em casa esta noite.

     Se eu ficar em casa esta noite, então a geladeira ficará vazia.

     Se meu irmão ficar em casa esta noite, então a geladeira ficará vazia.

     Logo, a geladeira ficará vazia.

   Ex.: $S \vee D, S \rightarrow F, D \rightarrow F \vdash F$

   Prova:

1	$S \vee D$	P
2	$S \rightarrow F$	P
3	$D \rightarrow F$	P
4	F	$1,2,3 \vee E$

7. Introdução do Bicondicional ($\leftrightarrow I$): De quaisquer fbfs de formas $(A \rightarrow B)$ e $(B \rightarrow A)$, podemos inferir $A \leftrightarrow B$.

8. Eliminação do Bicondicional ($\leftrightarrow E$): De qualquer fbf da forma $A \leftrightarrow B$, podemos inferir $A \rightarrow B$ ou $B \rightarrow A$.

   Exemplo:

   - Se houver um terremoto, então a cidade será destruída, E se a cidade for destruída, então é porque houve um terremoto.

     A cidade será destruída SE E SOMENTE SE houver um terremoto.

   Ex.: $P \leftrightarrow Q \vdash Q \leftrightarrow P$

Prova:

1	$P \leftrightarrow Q$	P
2	$P \rightarrow Q$	$1 \leftrightarrow E$
3	$Q \rightarrow P$	$1 \leftrightarrow E$
4	$Q \leftrightarrow P$	$2,3 \leftrightarrow I$

9. Prova do Condicional (PC): Dada uma derivação de uma fbf A a partir de uma hipótese B, podemos descartar a hipótese e inferir $B \rightarrow A$. [2]

   Ex.: $I, (I \wedge C) \rightarrow \neg S, \neg S \rightarrow \neg A \vdash C \rightarrow \neg A$

   Prova:

1	I	P
2	$(I \wedge C) \rightarrow \neg S$	P
3	$\neg S \rightarrow \neg A$	P
4	C	H(Hipótese)
5	$I \wedge C$	$1,4 \wedge I$
6	$\neg S$	$2,5MP$
7	$\neg A$	$3,6MP$
8	$C \rightarrow \neg A$	$4,7PC$

10. Redução ao Absurdo (RAA): Dada uma derivação de uma contradição a partir de uma hipótese A, podemos descartar a hipótese e inferir $\neg A$.[3]

    Ex.: $P \rightarrow Q, \neg Q \vdash \neg P$

    Prova:

1	$P \rightarrow Q$	P
2	$\neg Q$	P
3	P	H
4	Q	$1,3MP$
5	$Q \wedge \neg Q$	$2,4 \wedge I$
6	$\neg P$	$3,5RAA$

Regras Derivadas

[2] A Prova do Condicional é também chamada de Teorema da Dedução e é normalmente utlizada se o conseqüente é da forma $A \rightarrow B$. Nestes casos, A é tomado como uma premissa adicional e se infere B das premissas dadas e de A.

[3] Contradição é qualquer fbf da forma $A \wedge \neg A$.

1. Modus Tollens (MT): De fbfs da forma $A \rightarrow B$ e $\neg B$, infere-se $\neg A$.

   Exemplos:

   - Se meu carro estiver no estacionamento, então estou na Universidade.

     Eu não estou na Universidade.

     Logo, meu carro não estã no estacionamento.

   - Se meu animal de estimação for um gato ou um cão, então ele será um mamífero.

     Meu animal de estimação não é um mamífero.

     Logo, ele não é um cão nem um gato.

2. Silogismo Hipotético (SH): De fbfs da forma $A \rightarrow B$ e $B \rightarrow C$, infere-se $A \rightarrow C$.

   Exemplos:

   - Se o pássaro está perdido, então a porta da gaiola está aberta.

     Se a porta da gaiola está aberta, então o pássaro pode retornar à gaiola.

     Logo, se o pássaro está perdido, então ele pode retornar à gaiola.

   - Se meu time jogar bem, então ele vencerá as suas partidas.

     Se meu time vencer as suas partidas, então ele se classificará para as finais do campeonato.

     Logo, se meu time jogar bem, então ele se classificará para as finais do campeonato.

3. Regra da Absorção (ABS): De uma fbf da forma $A \rightarrow B$, infere-se $A \rightarrow (A \wedge B)$.

4. Regra do Dilema Construtivo (DC): De fbfs da forma $A \vee B$, $A \rightarrow C$ e $B \rightarrow D$, infere-se $C \vee D$.

   Exemplo:

   - A festa será na minha casa ou na sua.

     Se fizermos a festa em minha casa, então minha casa ficará uma bagunça.

     Se fizermos a festa em sua casa, então sua casa ficará uma bagunça.

     Logo, ou a minha casa ou a sua ficará uma bagunça.

5. Regra da Repetição (RE): De qualquer fbf A, infere-se A.

6. Regra do Silogismo Disjuntivo (SD): De fbfs da forma $A \vee B$ e $\neg A$, infere-se B.

   Exemplo:

   - Ou o cachorro está dentro de casa ou ele está no pátio.
     O cachorro não está no pátio.
     Logo, o cachorro está dentro de casa.

Exercícios:

1. Se há um jogo de futebol na Ressacada, então viajar de avião é diícil. Se eles chegarem no horário no aeroporto, então a viagem de avião não será difícil. Eles chegaram no horário, portanto não houve jogo na Ressacada.

   Sejam:
   P: Existe um jogo de futebol na Ressacada.
   Q: Viajar é difícil.
   R: Eles chegaram no aeroporto no horário.

   $P \rightarrow Q, R \rightarrow \neg Q, R \vdash \neg P$

   Prova:

1	$P \rightarrow Q$	P
2	$R \rightarrow \neg Q$	P
3	R	P
4	$\neg Q$	$2,3 MP$
5	$\neg P$	$1,4 MT$

2. Verifique se os argumentos a seguir constituem argumentos válidos.

   (a) Se este animal for um pássaro, então ele tem sangue-quente.
   Se este animal for um réptil, então ele terá sangue-frio.
   Este animal possui ou sangue-quente ou sangue-frio.
   Logo, este animal é um pássaro ou um réptil.

   (b) Se João está em casa, então a porta está aberta.
   A porta está aberta.
   Logo, João está em casa.

   (c) Se vocês dois ficarem em casa, então poderei sair sossegado.
   Vocês dois vão ficar em casa.
   Logo, poderei sair sossegado.

3. Determine se as seguintes formas são válidas ou inválidas:

   (a) $P \rightarrow Q, R \rightarrow \neg Q, R \vdash \neg P$.

   (b) $A \rightarrow (B \vee C), B \rightarrow \neg A, D \rightarrow \neg C \vdash A \rightarrow \neg D$.

   (c) $B \wedge C, (B \leftrightarrow C) \rightarrow (H \vee G) \vdash H \vee G$.

   (d) $(Q \wedge R) \rightarrow P, \neg Q, \neg R \vdash \neg P$.

   (e) $P \rightarrow Q, (\neg Q \vee R) \wedge \neg R, \neg(\neg P \vee S) \vdash \neg S$.

2.3.8 Tabelas-Verdade como Forma de Validação

Um argumento de validação é válido se e somente se todas as suas instâncias são válidas. Uma instância de um argumento é válida se for impossível que sua conclusão seja falsa enquanto suas premissas forem verdadeiras. Isto é, se não houver situação na qual a sua conclusão é falsa enquanto as suas premissas são verdadeiras. Uma Tabela-Verdade é uma lista exaustiva de de situações possíveis. Daí podermos utilizar a tabela-verdade para determinar se a forma é ou não válida.

Se a forma for válida (pela definição, uma forma válida é aquela em que todas as instâncias são válidas), então qualquer instância dela deve ser válida. Assim, podemos utilizar tabelas-verdade para estabelecer a validade não apenas de argumentos,mas de argumentos específicos.

Por exemplo, consideremos o Silogismo Disjuntivo:
- A Princesa ou a Rainha comparecerá à cerimônia.
- A Princesa não comparecerá.
- $\vdash$ A Rainha comparecerá.

$P \vee Q, \neg P \vdash Q$

P	Q	$P \vee Q$	$\neg P$	$\vdash Q$
V	V	V	F	V
V	F	V	F	F
F	V	V	V	V
F	F	F	V	F

A forma é inválida se existirem premissas verdadeiras e conclusão falsa. Neste caso, existem quatro sitiações possíveis e somente na terceira as premissas são verdadeiras. Mas neste caso, a conclusão também é verdadeira. A tabela mostra que o argumento é válido.

Exercícios: Determine se a conclusão C pode ser logicamente obtida através das premissas $H_1 e H_2$.

1. $H_1 : P \rightarrow Q, H_2 : P, C : Q$
2. $H_1 : P \rightarrow Q, H_2 : \neg P, C : Q$
3. $H_1 : P \rightarrow Q, H_2 : \neg(P \wedge Q), C : \neg P$
4. $H_1 : \neg P, H_2 : P \leftrightarrow Q, C : \neg(P \wedge Q)$
5. $H_1 : P \rightarrow Q, H_2 : Q, C : P$

2.4 Cálculo de Predicados

Até este momento, examinamos a lógica simbólica considerando apenas proposições. As técnicas de inferência se restringiam a suposição de que as premissas e as conclusões fossem proposições.

No entanto, a lógica proposicional possui um poder de representação limitado, não sendo suficiente para expressar muitas coisas óbvias e elementares, por exemplo, o fato de duas fórmulas atômicas possuírem algumas características em comum. Para isto, se introduz o conceito de Predicado em uma fórmula atômica.

A lógica que se baseia na análise dos predicados em qualquer proposição é chamada Lógica de Predicados. A Lógica de Predicados se preocupa em introduzir noções lógicas para expressar qualquer conjunto de fatos através de três tipos de expressões: termos, predicados e quantificadores.

Cálculo de Predicados é a extensão do Cálculo Proposicional em que se consideram variáveis e quantificadores sobre variáveis. Os dois quantificadores mais importantes são o quantificador universal e o existencial, respectivamente representados pelos símbolos $\forall e \exists$.

2.4.1 Algumas Definições

- **Classe de Atributos:** Eles são representados pelos substantivos comuns, locuções nominais, adjetivos, locuções adjetivas, verbos e locuções verbais.

  Exemplo:

  Todos os homens são mortais

  Sócrates é um homem

  Então, Sócrates é mortal.

  Que pode ser representado por:

$\forall x(H(x) \rightarrow M(x))$

$H(s)$

$\vdash M(s)$

onde H, M e s não são sentenças, como na Lógica Proposicional, mas classes de atributos.

- **Quantificadores:** São operadores lógicos, mas em vez de indicarem relações entre sentenças, eles expressam relações entre conjuntos designados pelas classes de atributos lógicos. Eles são classificados de universais e existenciais.

  - Quantificador Universal ($\forall$): Este tipo de quantificador é formado pelas expressões "todo" e "nenhum".
    Ex.:

    * Todo Homem é Mortal, ou seja, qualquer que seja x, se x é Homem, então x é Mortal. $\forall x(H(x) \rightarrow M(x))$
    * Nenhum Homem é Vegetal, ou seja, qualquer que seja x, se x é Homem, então x NÃO é Vegetal. $\forall\ x\ (H(x)\ \rightarrow\ \neg\ V(x))$

  - Quantificador Existencial ($\exists$): Este tipo de quantificador é formado pelas expressões "existe algum" ou "pelo menos um" ou ainda "para algum".
    Ex.:

    * Pelo menos um Homem é Inteligente, ou seja, existe pelo menos um x em que x seja Homem e x seja Inteligente. $\exists\ x\ (H(x)\ \wedge\ I(x))$

  - **Predicados:** Descrevem alguma coisa ou características de um ou mais objetos. Eles serão denotados por letras maiúsculas.
    Ex.:

    Bob ama Cathy : $A(b, c)$

    Bob ama alguém : $\exists x A(b, x)$

    Bob ama a todos : $\forall x A(b, x)$

2.4.2 Sintaxe do Cálculo de Predicados

Elementos Válidos da Linguagem

- Símbolos Lógicos:

  - Operadores Lógicos: $\neg, \wedge, \vee, \rightarrow, \leftrightarrow$;

- Quantificadores: $\forall, \exists$;
- Parênteses: $(,)$.

- Símbolos Não-Lógicos:
  - Letras Nominais: letras minúsculas de "a" a "t";
  - Variáveis: letras minúsculas de "u" a "z";
  - Letras Predicativas: letras maiúsculas.

- Fórmulas Atômicas
  - É uma letra predicativa seguida por zero ou mais letras nominais.

- Fórmula Bem Formada
  - Uma fórmula atômica é uma fórmula bem formada (fbf);
  - Se P é uma fbf, então ¬P também o é;
  - Se P e Q são fbfs, então: $(P \wedge Q), (P \vee Q), (P \rightarrow Q) e (P \leftrightarrow Q)$ também o são;
  - Se $\Phi(a)$ é uma fbf contendo uma letra nominal a, então qualquer forma $\forall x \Phi(x)$ é uma fbf onde $\Phi(x)$ é o resultado de se substituir uma ou mais ocorrências de a em Φ por uma variável x, que não ocorra em Φ.
    Exemplos: Seja $P = F(a) \wedge G(a, b)$, então são fbfs:
    $\forall x(F(x) \wedge G(a, b))$
    $\forall x(F(x) \wedge G(x, b))$
    $\forall x(F(a) \wedge G(a, x))$
    $\exists x(F(x) \wedge G(a, b))$

2.4.3 Regras de Inferência para o Cálculo de Predicados

Todas as regras definidas no Cálculo Proposicional são utlizadas para o Cálculo de Predicados, apenas referenciando-as para os quantificadores. Além disso, para o Cálculo de Predicados, com respeito as regras de inferência, são inseridas mais algumas que serão vistas adiante.

Exemplo: $\neg F(a) \vee \exists x F(x), \exists x F(x) \rightarrow P \vdash F(a) \rightarrow P$.

Prova:

1	$\neg F(a) \vee \exists x F(x)$	P
2	$\exists x F(x) \rightarrow P$	P
3	$F(a)$	H (Hipótese para PC)
4	$\neg\neg F(a)$	$3DN$
5	$\exists x F(x)$	$1, 4SD$
6	P	$2, 5MP$
7	$F(a) \rightarrow P$	$3, 6PC$

Regras Básicas

1. Eliminação Universal (EU): De uma fbf quantificada universalmente $\forall x \Phi(x)$, infere-se uma fbf da forma $\Phi(a)$, a qual resulta de se substituir cada ocorrência da variável x em Φ por uma letra nominal a. Esta regra é, as vezes, chamada de Instanciação Universal.

   Ex.: $\forall x(H(x) \rightarrow M(x)), H(s) \vdash M(s)$

   Prova:

1	$\forall x(H(x) \rightarrow M(x))$	P
2	$H(s)$	P
3	$H(s) \rightarrow M(s)$	$1EU$
4	$M(s)$	$2, 3MP$

2. Introdução Universal (IU): De uma fbf contendo uma letra nominal a, que não ocorre em qualquer premissa ou em qualquer hipótese vigente na linha em Φ ocorre, infere-se uma fbf da forma $\forall x \Phi(x)$, onde $\Phi(x)$ é o resultado de se substituir todas as ocorrências de a em Φ por uma variável x que não ocorra em Φ.

   Ex.: $\forall x(P(x) \rightarrow C(x)), \forall\ x\ (C(x)\ \rightarrow\ V(x)) \vdash \forall\ x\ (P(x)\ \rightarrow\ V(x))$

   Prova:

1	$\forall x(P(x) \rightarrow C(x))$	P
2	$\forall x(C(x) \rightarrow V(x))$	P
3	$P(a) \rightarrow C(a)$	$1EU$
4	$C(a) \rightarrow V(a)$	$1EU$
5	$P(a) \rightarrow V(a)$	$3, 4SH$
6	$\forall x(P(x) \rightarrow V(x)$	$5IU$

3. Introdução Existencial (IE): Dada uma fbf Φ contendo uma letra nominal a, infere-se uma fbf da forma $\exists x\Phi(x)$, onde $\Phi(x)$ é o resultado de se substituir uma ou mais ocorrências de a em Φ por uma variável x que não ocorra em Φ. Entre as restrições apresentadas para a utilização da IE ressalta-se:

   - a pode ocorrer em uma hipótese, não utilizada ainda, ou em uma premissa;
   - a variável x não precisa substituir todas as ocorrências de a em Φ, é preciso substituir somente uma ou mais;
   - IE permite introduzir somente um quantificador existencial por vez e somente do lado esquerdo da fórmula.

   Ex.: $\forall x(F(x) \vee G(x)) \vdash \exists x(F(x) \vee G(x))$

   Prova:

1	$\forall x(F(x) \vee G(x))$	P
2	$F(a) \vee G(a)$	EU
3	$\exists x(F(x) \vee G(x)$	$2IE$

4. Eliminação Existencial (EE): Dada uma fbf quantificada existencialmente $\exists x\Phi(x)$ podemos inferir $\Phi(a)$, contanto que a letra nominal não ocorra em $\Phi(x)$, nem em qualquer premissa, nem em qualquer hipótese e nem em qualquer passo anterior da derivação. Estas restrições podem ser facilmente satisfeitas escolhendo uma nova letra nominal cada vez que a Eliminação Existencial for aplicada.

   Ex.: $\exists x(F(x) \wedge G(x)) \vdash \exists x(F(x))$

   Prova:

1	$\exists x(F(x) \wedge G(x))$	P
2	$F(a) \wedge G(a)$	$1EE$
3	$F(a)$	$2 \wedge E$
4	$\exists xF(x)$	$3IE$

Regras Derivadas

- Itercâmbio de Quantificadores
  - $\neg(\forall x \neg F(x)) = \exists xF(x)$

- $\neg(\forall x F(x)) = \exists x \neg F(x)$
- $\forall x \neg F(x) = \neg(\exists x F(x))$
- $\forall x F(x)) = \neg(\exists x \neg F(x))$

Exercícios:

1. Mostre que:

   (a) $\forall\ x\ H(x)\ \rightarrow\ M(x), \exists\ x\ H(x) \vdash\ \exists\ x\ M(x)$

   Prova:

1	$\forall H(x) \rightarrow M(x)$	P
2	$\exists x H(x)$	P
3	$H(a)$	H Hipótese para EE
4	$H(a) \rightarrow M(a)$	$1EU$
5	$M(a)$	$3, 4MP$
6	$\exists\ x\ M(x)$	IE
7	$\exists\ x\ M(x)$	$1, 3-6EE$

   (b) $\exists\ x\ P(x)\ \wedge\ \forall\ x\ Q(x) \vdash\ \exists\ x\ (P(x)\ \wedge\ Q(x))$

   (c) $\forall\ x\ (\neg\ P(x)\ \rightarrow\ Q(x)),\ \forall\ x\ \neg\ Q(x) \vdash\ P(a)$

2. Verifique se as seguintes formas são válidas ou inválidas.

   (a) $\exists\ x\ (P(x)\ \wedge\ Q(x))\ \vdash\ \exists\ x\ P(x)\ \wedge\ \exists\ x\ Q(x)$

   (b) $\exists\ x\ P(x)\ \wedge\ \exists\ x\ Q(x)\ \vdash\ \exists\ x\ (P(x)\ \wedge\ Q(x))$

3. Considerando as seguintes informações:

   - Toda atriz é bonita.

   - As avós não são bonitas.

   - Algumas avós são inteligentes.

   Provar que:

   - Vão existir mulheres que são inteligentes e não são atrizes.

Capítulo 3

Teoria dos Conjuntos

3.1 Origens da Teoria dos Conjuntos

A história da Teoria dos Conjuntos difere um pouco da maioria das outras áreas da Matemática, para as quais um longo processo de evolução de idéias, geralmente envolvendo várias pessoas trabalhando em paralelo, pode ser traçado. No caso da Teoria dos Conjuntos, pode-se dizer que ela é criação de uma única pessoa: Georg Cantor.

Foi com o trabalho de Cantor que a Teoria dos Conjuntos conseguiu finalmente receber um tratamento matemático adequado. os primeiros trabalhos de Cantor eram sobre a Teoria dos Números, e ele publicou vários artigos sobre este assunto. Estes artigos, no entanto, não davam nenhuma indicação de que Cantor iria alterar todo o curso da moderna matemática. Porém, em 1872, em uma viagem à Suiça, Cantor conheceu Richard Dedekind. Por seu profundo pensamento abstrato e lógico, Dedekind teve grande influência nas idéias desenvolvidas por Cantor. Em 1874 Cantor publicou um artigo no *Crelle's Journal* que representou o nascimento da Teoria dos Conjuntos. Neste artigo, Cantor defendia a idéia de que existiriam pelo menos dois tipos de "infinito". Ele demostrou que os números reais algébricos poderiam ser colocados em uma correspondência de um-para-um com os números naturais, enquanto que com os números reais esta correspondência não existiria.

Em seus artigos seguintes, Cantor introduziu a idéia de equivalência de conjuntos e estabeleceu que dois conjuntos seriam equivalentes, ou possuiriam a mesma potência, se pudesse se estabelecer uma correspondência de um-para-um entre estes conjuntos.

Neste capítulo introduziremos os conceitos elementares de teoria dos Conjuntos. Apesar da apresentação ser, até certo ponto, de maneira informal, tentaremos apre-

sentar provas formais que utilizem as técnicas apresentadas no capítulo anterior. A medida que formos prosseguindo em nosso estudo, procuraremos enfatizar analogias entre o Cálculo Proposicional e as Operações sobre Conjuntos.

3.2 Conceitos Primeiros

Enquanto na Geometria Euclidiana costuma-se adotar, sem definição, as noções de ponto, reta e plano, na Teoria dos Conjuntos as noções consideradas primitivas são as seguintes:

a) Conjunto

b) Elemento

c) Pertinência entre Elemento e Conjunto

d) Conjunto Universo

Definimos numa meta-linguagem os conceitos chamados "conceitos primeiros", que são explicáveis mas não definidos. Os conceitos primeiros nos dão a noção de universo (representando todas as coisas), conjunto, elemento e pertinência.

$$< U, X, x, \in >$$

3.2.1 Noção de Conjunto

A noção de conjunto, intuitivamente, pode ser designada como toda coleção bem definida de objetos, não importa de que natureza, considerados globalmente [1][10].

A noção matemática de conjunto é praticamente a mesma que se usa na linguagem comum, onde, normalmente, se associa a idéia de conjunto a uma coleção de objetos de qualquer natureza, portanto, pode-se exemplificar outros conjuntos:

1. conjunto de livros em uma biblioteca,
2. conjunto de letras da palavra "Matemática",
3. conjunto de lobos em uma matilha,
4. conjunto de catarinenses,
5. conjunto de números naturais,

6. conjunto de números reais tal que $x^2 - 4 = 0$

De modo geral, pensamos em conjuntos como uma coleção de objetos que compartilham de alguma propriedade em comum. Por exemplo, em matemática é bastante comum considerarmos um conjunto de linhas, um conjunto de triângulos, etc. No entanto, é importante ressaltar que esta característica comum entre os elementos não é necessária, e um conjunto que consista de objetos como: um carro, o número 3, uma porta e o aluno João também é um exemplo aceitável de conjunto.

A notação de conjuntos geralmente utiliza letras maiúsculas:

$$A, B, C, \ldots X, Y, Z$$

3.2.2 Elementos

Os objetos que constituem um conjunto denominam-se elementos do conjunto. Por exemplo:

- José é um elemento do conjunto de catarinenses,
- 1 é elemento do conjunto de números naturais,
- -2 é elemento do conjunto dos números reais que satisfaz à equação $x^2 - 4 = 0$.

Os elementos dos conjuntos são geralmente denotados por letras minúsculas:

$$a, b, c, \ldots x, y, z$$

Assim o conjunto A cujos elementos são a, b, c é denotado por:

$$A = \{a, b, c\}$$

3.2.3 Relação de Pertinência

Um conceito fundamental da Teoria dos Conjuntos é o de "ser membro" ou "pertencer" a um conjunto. Qualquer objeto que faça parte de um conjunto é chamado um "membro" ou um "elemento" daquele conjunto. Um conjunto é dito "bem-definido" ser for possível determinar, através de certas regras, se um dado objeto é membro de um conjunto.

Para denotar que o elemento x pertence ao conjunto X utiliza-se:

$$x \in X$$

que é lido como "x é um elemento de X", ou "x pertence a X", ou ainda "x está em X".

Se o elemento x não pertence ao conjunto X denota-se:

$$x \notin X$$

que é equivalente à negação da proposição "x está em X", ou seja?

$$\neg(x \in X) = x \notin X$$

Esta notação é devida ao matemático italiano Giuseppe Peano (1858- 1932)[10].

É importante ressaltar que nenhuma restrição foi colocada sobre que objetos podem ser membros de um conjunto. Não é raro termos conjuntos cujos membros são também conjuntos, tais como:

$$S = \{a, \{1, 2\}, p, \{q\}\}$$

No entanto, é importante distinguir entre o conjunto $\{q\}$ que é um elemento de S e o elemento q, que é um membro de $\{q\}$ mas não é um membro de S.

3.2.4 Conjunto Universo

Segundo Alencar [1] as palavras "elemento" e "conjunto" têm muitas vezes significado relativo, pois um mesmo ente pode ser elemento *em relação* a certos entes e conjunto *em relação* a outros entes. Assim, por exemplo, uma *turma* de um colégio é um *elemento* do conjunto das turmas do colégio, mas também é um conjunto de alunos do colégio; analogamente uma reta é um *elemento* do conjunto de todas as retas, mas também é um conjunto de pontos, etc.

Nestas condições, para o rigor matemático, deve-se observar quais são os entes considerados como *elementos*. Assim, por definição chama-se *conjunto universo* ou simplesmente *universo* de uma teoria, o conjunto de todos os entes que são sempre considerados como elementos nesta teoria [1]. Assim, por exemplo, na Aritmética, o universo é o conjunto de todos os números inteiros não negativos $\{0, 1, 2, 3, ...\}$ e em Geometria, o universo é o conjunto de todos os pontos, ou seja , o espaço.

Geralmente, o conjunto universo de uma teoria é denotado pela letra U. Num diagrama de Venn, os elementos do universo U são geralmente representados por

pontos internos a um quadrado (ou retângulo) e os demais conjuntos são representados por círculos contidos no quadrado (ou retângulo).

Exemplo 3.2.1 *A declaração type em PASCAL especifica que o conjunto universo Alfabeto é o conjunto de todos caracteres no teclado, tais como* **A**, **7**, *e* %.

type

Alfabeto = **set of** char;

3.3 Conjuntos Numéricos

É conveniente padronizar certos conjuntos de números usuais na teoria dos conjuntos. São particularmente importantes os seguintes conjuntos numéricos:

a) Conjunto dos números naturais

$$\mathcal{N} = \{1, 2, 3, 4, ...\}$$

b) Conjunto dos números inteiros

$$\mathcal{Z} = \{..., -3, -2, -1, 0, 1, 2, 3, ...\}$$

ou

$$\mathcal{Z} = \{0, 1, 2, 3, ...\}$$

c) Conjunto dos números racionais Q. Seus elementos são todos os números que podem ser colocados na forma p/q, em que $p \in \mathcal{Z}$ e $q \neq 0$ e $q \in \mathcal{Z}$.

d) Conjunto dos números reais $\Re$ são todos os números racionais e não racionais.

e) Conjunto dos números complexos $\mathcal{C}$ tem seus elementos números da forma $a + bi$, com $a \in \Re$, $b \in \Re$ e $i = \sqrt{-1}$.

3.4 Diagrama de Venn

A fim de facilitar o entendimento de certas definições e demonstrações da Teoria dos Conjuntos, é muito útil a representação de um conjunto por um recinto plano delimitado por uma linha fechada qualquer, não entrelaçada [1]. Esta representação pictográfica recebe o nome de diagrama de Venn. No diagrama de Venn 3.1, os elementos do conjunto indicam-se por pontos *internos* ao recinto, e elementos que não pertencem ao conjunto são representados por pontos *externos* ao mesmo recinto.

Existem várias outras maneiras de se descrever um conjunto:

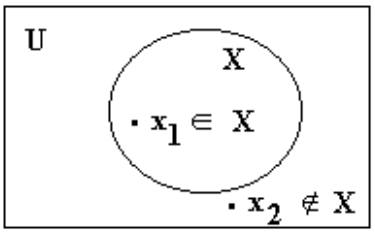

Figura 3.1: Diagrama de Venn

- listar (ou listar parcialmente) seus elementos,
- usar recursão para descrever como gerar seus elementos ou,
- descrever uma propriedade P que caracteriza seus elementos.

Exemplo 3.4.1 *Um conjunto particular S pode ser descrito pela sua propriedade característica:*

$$S = \{x | x \, par \, inteiro \, positivo\}$$

Isto é lido como "o conjunto de todo x tal que x é par inteiro positivo".

Ou ainda, usando a notação da Lógica de Predicados:

$$\forall x S(x) = \forall x, x \in S$$

3.5 Propriedades dos Conjuntos

Definição 3.5.1 Subconjunto: *Intuitivamente, pode-se dizer que é o conjunto que está dentro de outro conjunto conforme figura 3.2. Sejam X e Y quaisquer dois conjuntos. Se todo elemento de X for também um elemento de Y, então X é chamado de subconjunto de Y.*

$$X \subseteq Y \leftrightarrow \forall x (x \in X \rightarrow x \in Y) \leftrightarrow Y \supseteq X$$

Voltando ao exemplo 3.2.1, agora os subconjuntos podem ser definidos como variáveis no programa PASCAL pelas declarações:

var

Iniciais: Alfabeto; Letras: Alfabeto;

Em seguida são determinadas estas variáveis:

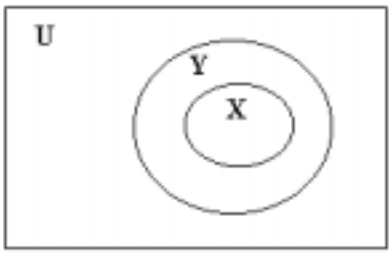

Figura 3.2: Representação de subconjunto

Iniciais := ['A' .. 'F']; Letras := ['C' .. 'G'];

Onde, os pontos fazem a ordenação (no caso alfabética) e os colchetes são usados para denotar conjuntos em PASCAL. Após a determinação, a variável *Iniciais* tem o valor $\{A, B, C, D, E, F\}$ e *Letras* tem o valor $\{C, D, E, F, G\}$. A enumeração ordenada é conveniente para especificar quais elementos são membros do conjunto, mas devido estes serem conjuntos indexados, a ordem dos elementos não é importante e pode a seqüência *Iniciais := ['B','A','D','F','E','C']* ter o mesmo valor que a determinada anteriormente. Devido ao conjunto não ser ordenado, os elementos deste conjunto não podem ser referenciados, assim não pode-se examinar o "terceiro" elemento do conjunto *Iniciais* [6].

Definição 3.5.2 Inclusão: *A relação de pertinência é uma relação entre elemento e conjunto [8]. A relação de inclusão é uma relação entre conjuntos. Pela relação de inclusão dois conjuntos podem ser comparados. Diz-se que um conjunto X está contido num conjunto Y se e somente se todo elemento de X é também um elemento de Y. Simbolicamente tem-se*

$$X \subset Y \leftrightarrow \forall x(x \in X \rightarrow x \in Y)$$

Definição 3.5.3 Igualdade de conjuntos: *Dois conjuntos X e Y são iguais quando todo elemento de X pertence também a Y e, reciprocamente, todo elemento de Y pertence a X. Simbolicamente tem-se:*

$$X = Y \leftrightarrow \forall x(x \in X \leftrightarrow x \in Y)$$

- $X = \{a, e, i, o, u\}$ e $Y = \{e, o, i, a, u\}$
- $X = \{0, 1, 2, 3, ...100\}$ e $Y = \{x | x$ é inteiro e $0 \leq x \leq 100\}$

- $X = \{x | x^2 = x\}$ e $Y = \{0, 1\}$

Observa-se que na definição de igualdade entre conjuntos não intervém a noção de ordem entre os elementos, portanto:

$$\{1, 2, 3\} = \{1, 3, 2\} = \{3, 2, 1\}$$

Definição 3.5.4 Desigualdade de Conjuntos: *Do mesmo modo se X não é igual a Y escreve-se $X \neq Y$, é evidente que existe elemento de X que não pertence a Y ou existe elemento em Y que não pertence a X.*

Exemplo 3.5.1 *Exemplos de conjuntos desiguais são:*

- $\{1, 2, 3, 4\} \neq \{2, 3, 4, 5\}$
- $\{a, b, c\} \neq \{a, a, b, e\}$
- $\{frango, pato, galinha\} \neq \{frango, pato, marreco\}$

Definição 3.5.5 Subconjunto Próprio: *Um conjunto X é chamado Subconjunto Próprio de um conjuto Y se:*

$$X \subseteq Y \wedge X \neq Y$$

Ou seja, existe elemento de Y que não pertence a X, isto e; além de todo elemento de X pertencer a Y, tem também elemento de Y que não pertence a X.

É importante ressaltar as diferenças entre pertinência e inclusão. Podemos ilustrar esta diferença com o exemplo a seguir:

$$A = \{1, 2, 3\}, B = \{1, 2\}, C = \{1, 3\}, D = \{3\}$$

então

$$B \subseteq A, C \subseteq A, D \subseteq A$$

ou

$$\{1, 2\} \subseteq \{1, 2, 3\}, \{1, 3\} \subseteq \{1, 2, 3\} e \{3\} \subseteq \{1, 2, 3\}$$

Por outro lado, $1 \in \{1, 2, 3\}$ e não 1 está incluso em $\{1, 2, 3\}$. Apenas um conjunto pode estar incluído ou ser subconjuto de outro conjunto.

As propriedades a seguir representam importantes propriedades da inclusão de conjuntos.

Para quaisquer conjuntos A, B e C:

$$A \subseteq A$$

(reflexiva)

$$(A \subseteq B) \wedge (B \subseteq C) \rightarrow (A \subseteq C)$$

(transitiva)

$\forall x(x \in A \rightarrow x \in B) \wedge \forall x(x \in B \rightarrow x \in C) \vdash \forall x(x \in A \rightarrow x \in C)$

$\forall x(A(x) \rightarrow B(x)) \wedge \forall x(B(x) \rightarrow C(x)) \vdash (A(x) \rightarrow C(x))$

Prova:

1	$\forall x(A(x) \rightarrow B(x))$	P
2	$\forall x(B(x) \rightarrow C(x))$	P
3	$A(a) \rightarrow B(a)$	$1EU$
4	$B(a) \rightarrow C(a)$	$1EU$
5	$A(a) \rightarrow C(a)$	$3,4SH$
6	$\forall x(A(x) \rightarrow C(x)$	$5IU$

3.6 Conjuntos Especiais

3.6.1 O Conjunto Vazio

Um conjunto que não contenha nenhum elemento é chamado de Conjunto Vazio. Um conjunto vazio é denotado por $\emptyset$.

3.6.2 O Conjunto Potência

Dado qualquer conjunto A, nós sabemos que o conjunto vazio $\emptyset$ e o conjunto A são ambos subconjuntos de A. Da mesma forma, para qualquer elemento a de A, o conjunto $\{a\}$ é um subconjunto de A. Estendendo o raciocínio, podemos considerar outros subconjuntos de A. Podemos definir todos os subconjuntos do conjunto A da seguinte forma:

Para um conjunto A, a coleção ou família de todos os subconjuntos da A é chamada Conjunto Potência de A. O Conjunto Potência de A é denotado por $\rho(A)$ ou 2^A, e é tal que

$$\rho(A) = 2^A = \{X | X \subseteq A\}$$

Consideremos alguns conjuntos finitos e seus conjuntos potência. O conjunto potência do conjunto vazio possui apenas o elemento $\emptyset$, portanto $\rho(\emptyset) = \{\emptyset\}$. Para um conjunto $S_1 = \{a\}$, o conjunto potência $\rho\{S_1\} = \{\emptyset, \{a\}\} = \{\emptyset, S_1\}$. Para $S_2 = \{a, b\}$, $\rho\{S_2\} = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$. Para $S_3 = \{a, b, c\}$, $\rho\{S_3\} = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$.

Podemos utilizar uma representação binária para representar distintamente os subconjuntos de um conjunto. Para isto, devemos primeiramente supor que os elementos são ordenados, o que até agora não foi colocado como condição para a definição de conjuntos. Esta ordenação é geralmente necessária para a representação de conjuntos em um computador. Suponhamos uma ordem arbitrária e a cada elemento associemos um rótulo que descreve a posição do elemento com relação aos outros elementos do conjunto.

Tomemos como exemplo o conjunto S_2 visto anteriormente, no qual a é o primeiro elemento e b é o segundo elemento. Os diversos subconjuntos do conjunto S_2 podem ser representados da seguinte maneira:

$$\emptyset = B_{00}, \{a\} = B_{10}, \{b\} = B_{01}, e\{a, b\} = B_{11}$$

onde os índices de B contém 1 ou 0 se a rsepectiva posição do conjunto original em relação ao subconjunto possuir o elemento ou não.

A notação acimo pode ser generalizada para designar subconjuntos de conjuntos que possuam n elementos distintos. Os índices determinantes dos subconjuntos variam na representação binária de 0 até 2^{n-1}. Note que devemos ter o cuidado de inserir tantos tantos 0's à esquerda da representação binária quantos forem necessários para formar n dígitos binários no total. Como ilustração tomemos o conjunto $S_6 = \{a_1, a_2, ..., a_6\}$. Os exemplos a seguir demonstram a utilização do método para determinar os elementos de qualquer subconjunto.

$$B_{111} = B_{000111} = \{a_4, a_5, a_6\}$$

$$B_{1100} = B_{001100} = \{a_3, a_4\}$$

3.7 Álgebra dos Conjuntos

Quando se faz operações nos conjuntos tem-se um novo conjunto. Se uma operação sobre os elementos de um conjunto produzir resultados (imagem) que também são

elementos do mesmo conjunto, então o conjunto é chamado de "fechado" para aquela operação e esta propriedade é chamada de propriedade de "fechamento". A definição de operações binárias e unárias implica que os conjuntos nos quais as operações são realizadas sejam fecgadas para estas operações. A união e a interseção são operações binárias, associativas. Já o complemento é uma operação unária.

3.7.1 Conceito de Operações unárias, binárias e n-árias

Como o nome indica as operações binárias são feitas entre dois elementos de um conjunto e as nárias entre vários elementos do conjunto. Uma operação unária é aquela feita com um único elemento do conjunto.

Definição 3.7.1 Operação Unária: *Para se ter uma operação unária em um conjunto S, deve ser verdade que para qualquer $x \in S$, existe a operação de inverso $x^{\star}$ que é única e pertencente a S.*

Exemplo 3.7.1 *Exemplos de operações unárias:*

- *Tomar o negativo de um número no conjunto $\mathcal{Z}$.*
- *O conectivo de negação é uma operação unária de conjuntos proposicionais. Se P é proposicional então $\neg P$ é sua negativa.*

Definição 3.7.2 Operação binária: *Uma operação é binária em um conjunto S se para cada par ordenado (x, y) de elementos de S, a operação $x \circ y$ sempre existe e pertence ao conjunto S.*

Exemplo 3.7.2 *Exemplos de operações binárias:*

- *Operações binárias no conjunto $\mathcal{Z}$: adição, subtração, e multiplicação.*
- *Quando desenvolve-se a adição de um par ordenado de inteiros (x, y), a operação $x + y$ existe e resulta unicamente em um número inteiro.*
- *A divisão não é uma operação binária em $\mathcal{Z}$ porque não existe $x \div 0$.*

Para estes exemplos, deve estar claro que $\circ$ (operação binária) ou $\star$ (operação unária) podem depender não só de sua definição mas também dos conjuntos envolvidos.

Exercício 3.7.1 *Identificar se as operações são unárias ou binárias nos seguintes conjuntos:*

- $x \circ y = x \div y$; $S =$ *conjunto de todos inteiros positivos*
- $x \circ y = x \div y$; $S =$ *conjunto de todos números racionais positivos*
- $x \circ y = x^y$; $S = \Re$
- $x^\star = \sqrt{x}$; $S =$ *conjunto de todos números reais positivos*
- $x^\star =$ *solução da eq.* $(x^\star)^2 = x$; $S = \mathcal{C}$

3.7.2 União

O conceito de união pode ser entendido como todos os elementos que são dos conjuntos X e Y "conjuntamente". Ou seja, os elementos pertencem tanto ao conjunto X como ao conjunto Y. Representa-se a união (conforme 3.3) como:

$$X \cup Y$$

, ou seja

$$X \cup Y = \forall x(x \in X \vee x \in Y)$$

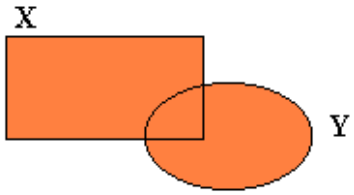

Figura 3.3: União de Conjuntos

3.7.3 Interseção

A interseção dos conjuntos X e Y é o conjunto de todos os elementos que pertencem ao conjunto X e ao conjunto Y. Representa-se a interseção como:

$$X \cap Y$$

, ou seja

$$X \cap Y = \forall x(x \in X \wedge x \in Y)$$

Quando a interseção $X \cap Y$ de dois conjuntos X e Y é o conjunto vazio, dizemos que estes conjuntos são "disjuntos". A figura 3.4 mostra a interseção entre dois conjuntos.

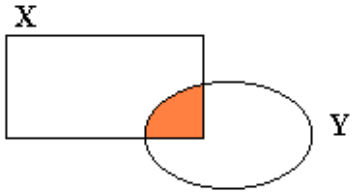

Figura 3.4: Interseção entre Conjuntos

3.7.4 Diferença

A diferença entre conjuntos X e Y é o conjunto de todos os elementos que pertencem ao conjunto X e não pertencem ao conjunto Y. Simbolicamente tem-se:

$$X - Y = \{x | x \in X \, e \, x \notin Y\} == \forall x (x \in X \wedge x \notin Y)$$

Exemplo 3.7.3 *A figura 3.5 ilustra através do diagrama a diferença entre dois conjuntos X e Y.*

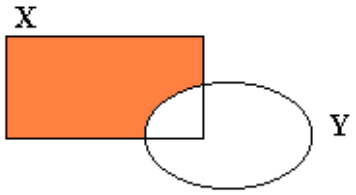

Figura 3.5: Diferença entre conjuntos

Exemplo 3.7.4 *Sejam os conjuntos $A = \{1, 3, 4, 5, 7\}$, $B = \{1, 3, 4, 5\}$ e $C = \{3, 5, 8, 9\}$. Tem-se:*

- $A - B = \{7\}$, $B - A = \emptyset$
- $B - C = \{1, 4\}$, $C - B = \{8, 9\}$

No exemplo 3.7.4 observa-se que $A - B$ é diferente de $B - A$ e $B - C$ é diferente de $C - B$, isto é *a diferença de conjuntos não é comutativa.*

3.7.5 Complemento

Seja U o conjunto Universo. Para qualquer conjunto X, o complemeneto de X, simbolicamente representado como $\sim X$ é composto por todo elemento x que pertencendo ao conjunto Universo, não pertença ao conjunto X, ou seja:

$$\sim X = U - X$$

3.8 Produto Cartesiano

Intuitivamente, o produto cartesiano de dois conjuntos é o conjunto de todos os pares ordenados dos elementos do primeiro conjunto que pode-se formar com os elementos do segundo conjunto.

Definição 3.8.1 *Supondo-se X e Y serem conjuntos de um universo U. O produto cartesiano de X e Y é denotado por $X \times Y$ e é definido por:*

$$X \times Y = \{(x, y) | x \in X \wedge y \in Y\}$$

Exemplo 3.8.1 *Dados os conjuntos $X_1 = \{a, b\}$ e $X_2 = \{1, 2\}$, o produto cartesiano $X_1 \times X_2$ é:*

$$X_1 \times X_2 = \{(a,1)(a,2)(b,1)(b,2)\}$$

A noção de produto cartesiano, definida para *dois* conjuntos, extende-se de maneira natural a qualquer número finito $n > 2$ de conjuntos.

Definição 3.8.2 *Chama-se* **produto cartesiano** *ou apenas* **produto** *dos n conjuntos $X_1, X_2, \ldots X_n$, pela ordem em que estão escritos, ao conjunto de todas as $n-uplas$ $(x_1, x_2, \ldots x_n)$ tais que $x_1 \in X_1$, $x_2 \in X_2$, $\ldots x_n \in X_n$.*

Este conjunto produto representa-se por uma das notações:

$$X_1 \, x \, X_2 \, x \ldots x \, X_n \text{ ou } \prod_{i=1}^{n} X_i$$

Os conjuntos $X_1, X_2, \ldots X_n$ dizem-se os *fatores* do produto cartesiano $X_1, X_2, \ldots X_n$, sendo X_1 o primeiro fator até X_n o né-simo fator.

Exercício 3.8.1 *Dados os conjuntos: $A = \{1, 2\}$ e $B = \{3, 4\}$. Obter: $A \times B$, $B \times A$, A^2 e A^3.*

3.9 Propriedades das Operações

3.9.1 Propriedade Associativa

Quaisquer que sejam os conjuntos X, Y e Z, tem-se que:

$$X \cup (Y \cup Z) = (X \cup Y) \cup Z$$

$$X \cap (Y \cap Z) = (X \cup Y) \cap Z$$

3.9.2 Propriedade Comutativa

Quaisquer que sejam os conjuntos X e Y, tem-se que:

$$X \cup Y = Y \cup X$$

$$X \cap Y = Y \cap X$$

3.9.3 Propriedade Distributiva

Quaisquer que sejam os conjuntos X, Y e Z, tem-se que:

$$X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z)$$

$$X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z)$$

A figura 3.6 mostra a distributividade.

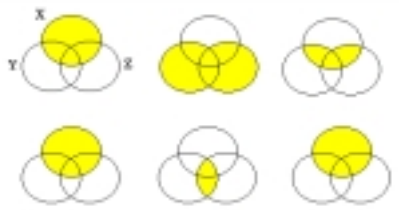

Figura 3.6: Distributividade

3.9.4 Propriedade Reflexiva

Qualquer que seja o conjunto X, tem-se que:

$$X \cup X = X$$

$$X \cap X = X$$

3.9.5 Propriedade de Fechamento

Quaisquer que sejam os conjuntos X e Y, então a união de X e Y, denotada por $X \cup Y$ e a interseção de X e Y denotada por $X \cap Y$, ainda são conjuntos no universo.

3.9.6 Elemento neutro para a união

O conjunto vazio $\emptyset$ é o elemento neutro para a união de conjuntos é tal que para todo conjunto X, se tem:

$$X \cup \emptyset = X$$

3.9.7 Elemento neutro para a interseção

O conjunto universo U é o elemento neutro para a interseção de conjuntos, tal que para todo conjunto X, tem-se:

$$X \cap U = X$$

3.9.8 Elemento nulo para a interseção

Se tomarmos a interseção do conjunto vazio $\emptyset$ com qualquer outro conjunto X, teremos o próprio conjunto vazio.

$$X \cap \emptyset = \emptyset$$

3.10 Cardinalidade de Conjuntos

3.10.1 Os Números Naturais

os conjuntos dos números naturais é um conjunto bastante conhecido e utilizado por muitas pessoas no seu dia-a-dia. Uma de suas utilizações mais freqüentes é para contar elementos e objetos. Esta utilização permite a definição da noção de similaridade ou equipotência de dois conjuntos e também do conceito de "número cardinal" de um conjunto. Deste modo podemos introduzir os conceitos de conjuntos finitos e infinitos, que são de grande importância na teoria dos autômatos.

Os Axiomas de Peano

O conjunto $\mathcal{N} = \{0, 1, 2, ...\}$ dos números naturais (incluido o zero) pode ser gerado iniciando-se com um conjunto vazio $\emptyset$ e a noção de "conjunto sucessor" de um

conjunto. Um "conjunto sucessor" é denotado por A^+ e definido como sendo o conjunto $A^+ = A \cup \{A\}$.

Seja $\emptyset$ o conjunto vazio e os seus conjuntos sucessores:

$$\emptyset^+, (\emptyset^+)^+, ((\emptyset^+)^+)^+, ...$$

que são:

$$\emptyset, \{\emptyset\}, \{\emptyset\{\emptyset\}\}, \{\emptyset, \{\emptyset\}, \{\emptyset\{\emptyset\}\}\}...$$

Se chamarmos de 0 o conjunto $\emptyset$, então $\emptyset^+ = 0^+ = 1, 1^+ = 0, 0^+ = 2$, e assim por diante, obteremos o conjunto $\{0, 1, 2, ...\}$.

podemos resumir dizendo que o conjunto dos números naturais pode ser obtido através da aplicação dos seguintes axiomas, conhecidos como Axiomas de Peano.

1. $0 \in \mathcal{N}$ (onde $0 = \emptyset$)
2. Se $n \in \mathcal{N}$, então $n^+ \in \mathcal{N}$ onde $n^+ = n \cup \{n\}$
3. Se um subconjuto $S \subseteq \mathcal{N}$ possui as propriedades:
   (a) $0 \in S$, e
   (b) se $n \in S$, então $n^+ \in S$

   então $S = \mathcal{N}$

3.10.2 Cardinalidade

Na seção anterior, nos preocupamos com a geração dos números naturais. vejamos agora, como utilizar o conjunto dos números naturais para contar. Através desta propriedade podemos medir o "tamanho" de um conjunto e "comparar" os tamanhos de quaisquer dois conjuntos.

A primeira questão que devemos examinar agora, diz respeito a como contar algo, seja o número de pessoas em uma sala, o número de livros em um estante, ou o número de elementos em um conjunto. O que devemos fazer, neste caso, é estabelecer uma correspondência de um-para-um entre os objetos a serem contados e o conjunto de naturais $\{1, 2, 3, ..., n\}$. Por esta correspondência dizemos que o número de objetos é n. generalizando esta técnica temos:

Definição 3.10.1 *Dois conjuntos A e B são ditos equipotentes (ou equivalentes, ou possuindo a mesma cardinalidade, ou ainda, similares), e denotados por $A \sim B$, se e somente se existir uma correspondência de um-para-um entre os elementos de A e os elementos de B.*

Exemplo 3.10.1 *Seja* $N = \{0, 1, 2, ...\}$ *e* $N_2 = \{0, 2, 4, ...\}$
Mostre que $N \sim N_2$.

Solução:
para cada elemento x *de* N, *corresponderá o elemento* $y = 2x$ *de* N_2. *Assim, podemos estabelecer uma correspondência de um-para-um entre* N *e* N_2 *e portanto* $N \sim N_2$. *Note também que* $N_2 \subset N$.

Podemos agora utilizar o conjunto dos números naturais para contar os elementos de um conjunto, ou seja, determinar seu número cardinal. Intuitivamente, um conjunto é finito se consiste de um número específico de elementos diferentes, isto é, se estabelecermos uma correspondência de um-para-um entre os elementos do conjunto e os elementos do conjunto dos números naturais, no qual o número 0 corresponde ao conjunto vazio, o número 1 corresponde ao primeiro elemento do conjunto, o número 2 corresponde ao segundo elemento do conjunto, e assim por diante, até o número n, que corresponde ao último elemento do conjunto. Dizemos então que o conjunto tem n elementos e que seu número cardinal é n.

Definição 3.10.2 *Dado um conjunto* X, *diz-se que* X *é finito se tem* n *elementos. O número* n *chama-se* número cardinal *do conjunto* X *e escreve-se* $n(X) = n$.

Os conjuntos podem ser finitos e infinitos. Diz-se que um conjunto é infinito se ele for equivalente a um subconjunto próprio.

Definição 3.10.3 *Qualquer conjunto cujo número cardinal é um número natural é um* conjunto finito. *Também, qualquer conjunto que não seja finito é chamado de* conjunto infinito.

Definição 3.10.4 *Qualquer conjunto equivalente ao conjunto dos números naturais é chamado de* enumerável.

Definição 3.10.5 *A cardinalidade de um conjunto enumerável é denotada pelo símbolo* $\aleph_0$ *chamado* aleph zero. *Utilizamos a notação* $n(X)$ *para denotar a cardinalidade de um conjunto finito* X.

Definição 3.10.6 *Todo conjunto finito ou enumerável é chamado de* contável.

O conjunto dos números reais, por exemplo, é infinito, porém, por ser compacto não pode se estabelecer uma correspondência de um-paraum com o conjunto dos números naturais e, portanto, ele é *não-enumerável*.

Definição 3.10.7 *Um conjunto que seja infinito e não enumerável é chamado de* incomensurável.

Cantor provou que o conjunto potência de um dado conjunto deve ser maior (cardinalidade maior) do que este conjunto e afirmou a existência de cardinalidade transfinita.

Exemplo 3.10.2 *Exemplos de conjuntos finitos:*

- *conjunto dos números de dias da semana*
- *conjunto de vogais*
- *conjunto de números de telefones de uma cidade*

Exemplo 3.10.3 *Exemplos de conjuntos infinitos:*

- *conjunto dos números naturais*
- *conjunto de átomos no universo*

3.11 Paradoxos na Teoria dos Conjuntos

Nesta seção são apresentados alguns paradoxos da Teoria dos Conjuntos. Maiores detalhes podem ser encontrados em [9] e [12].

3.11.1 Paradoxo de Cantor

O Paradoxo de Cantor diz que o conjunto de todos os conjuntos é seu próprio conjunto potência. Portanto, a cardinalidade do conjunto de todos os conjuntos deve ser maior do que ele mesmo. Seja $\mathcal{C}$ o conjunto de todos os conjuntos. Portanto, cada subconjunto de $\mathcal{C}$ é também um membro de $\mathcal{C}$. Assim, o conjunto potência de $\mathcal{C}$ é subconjunto de $\mathcal{C}$, isto é,

$$2^{\mathcal{C}} \subset \mathcal{C}$$

Mas $2^{\mathcal{C}} \subset \mathcal{C}$ implica em

$$\#(2^{\mathcal{C}} \leq \#(\mathcal{C})$$

contudo, de acordo com o teorema de Cantor

$$\#(\mathcal{C}) < \#(2^{\mathcal{C}})$$

Assim, o conceito de conjunto de todos os conjuntos conduz a uma contradição.

3.11.2 Paradoxo de Russel

Este paradoxo é devido ao filósofo e matemático britânico Bertrand Russell para ajudar a explicar o paradoxo que ele descobriu na teoria dos conjuntos. Primeira consideração: a maioria dos conjuntos não são elementos deles mesmos, mas alguns são. Por exemplo, o conjunto de todas as árvores não é uma árvore, nem o conjunto de todas as línguas não é uma língua. Todavia, uma lista de todas as listas (a qual é uma lista) ou o conjunto de todas as idéias abstratas, a qual é também é uma idéia abstrata.

Supondo-se agora que exista um conjunto S, o qual é composto de todos os conjuntos que *não são* elementos de si mesmos. Se S não é um elemento de si mesmo, então ele pertence a este conjunto. Mas, se S é um conjunto, então ele é um elemento de si mesmo e não pertence ao conjunto. Uma solução para este problema torna necessário que qualquer conjunto definido por um predicado também seja um sub-conjunto de um conjunto conhecido (a exceção deste é o conjunto potência). Desde que o conjunto de "conjuntos, os quais não são elementos deles mesmos" não é conhecido, deve ser feito primeiro um subconjunto de algum outro conjunto conhecido. Por exemplo, supondo-se U o conjunto dos conjuntos e A qualquer conjunto que pertence a U e não é elemento de si mesmo. Agora, S é definido como:

$$S = \{A \in U | A \notin A\}$$

A questão pode ser feita: S é um elemento de si mesmo? A resposta é não. Se $S \in S$, (S pertence ao conjunto dos conjuntos os quais não são elementos de si mesmos), ele satisfaz sua própria propriedade de definição e portanto $S \notin S$.

Em outras palavras S pertence ou não a si mesmo? Se S não pertence a S, então, pela definição de S, S pertence a si mesmo. Além disso, se S pertence a S, então pela definição de S, S não pertence a si mesmo. Em ambos os casos somos conduzidos a uma contradição [9].

Este paradoxo é semelhante ao Paradoxo do Barbeiro descrito na sub-seção 3.11.3.

3.11.3 Paradoxo do Barbeiro

Supondo-se que exista uma cidade onde um homem tenha uma barbearia. Este barbeiro deve barbear todos os homens e somente homens que não barbeiam a si mesmos. Quem barbeia o barbeiro ? Este paradoxo é conhecido como o paradoxo do barbeiro. Pensando que os homens desta cidade pertencem a dois conjuntos: o conjunto dos homens que barbeiam a si mesmos e o conjunto dos homens que não

barbeiam a si mesmos (não existe um terceiro conjunto!). Se o barbeiro pertence ao primeiro conjunto (homens que se barbeiam), descrito pelas circunstâncias, ele não se barbeia. Portanto, ele pertence ao segundo conjunto, então descrito pelas mesmas circunstâncias, ele deve barbear a si mesmo. A pergunta é se sim ou não. A única solução é que tal situação descrita acima não pode existir.

3.11.4 Paradoxo de Burali-Forti

Existe um paradoxo conhecido como Paradoxo de Burali-Forti atribuído a Cesare Burali-Forti. O Paradoxo diz respeito ao conjunto de "todos" números ordinais. Este conjunto deve ter um número ordinal o qual não está no conjunto, isto é o paradoxo existe desde que se diz conjunto de "todos" números ordinais. Segundo [12] intuitivamente, na teoria dos conjuntos cada conjunto ordenado tem um número ordinal. Além disso, o conjunto de todos os ordinais é ordenado, aonde este conjunto de todos ordinais tem um número ordinal dito $\mathcal{O}$. Mas o conjunto de todos os ordinais crescentes e incluindo qualquer ordinal dado é ordenado e portanto tem um número ordinal, o qual excede o ordinal dado em 1. Conseqüentemente, o conjunto de todos ordinais incluindo $\mathcal{O}$ tem o número ordinal $\mathcal{O} + 1$, o qual é maior do que $\mathcal{O}$. Portanto, $\mathcal{O}$ não é um número ordinal de "todos" ordinais.

3.11.5 Paradoxo de Gödel

Outro paradoxo mais moderno, seria o sobre Teorema da Incompleteza de Gödel. Um sistema de axiomas é completo quando todo teorema será verdade ou mentira. Se existir um sistema de axiomas consistentes (ou seja quando não existirem axiomas que entrem em contradição com outros axiomas) existirão sempre teoremas que se poderá provar que são mentiras e teoremas que se poderá provar que são verdades e outros que não se pode provar nada, nem que sejam verdades, nem que sejam mentiras. Neste caso, o sistema é dito incompleto, no sentido de que existem coisas que não se pode provar, nem que sejam verdades ou mentiras.

O Teorema de Gödel parte da premissa de que existem verdades e mentiras levando a conclusão que existem teoremas verdadeiros, falsos e outros que não se sabe se são verdades ou mentiras. Ou seja, partindo-se de duas verdades chegaria-se a um terceiro valor de verdade: *não sabido*. Este teorema pode ser interpretado como uma comprovação da lógica que utiliza conjuntos nebulosos (lógica "fuzzy").

Capítulo 4

Relações

4.1 Introdução

O conceito de uma relação é um conceito freqüentemente utilizado, seja no nosso dia-a-dia, seja na matemática. Associado ao conceito de relação está a ação de comparar objetos que estejam relacionados entre si. A capacidade de um computador de realizar operações diferentes baseado no resultado de comparações é, talvez, uma das características mais utilizadas durante a execução de um programa. Do mesmo modo, podemos dizer que bases de dados são compostas por relações entre conjuntos e a manipulação da base para extração de novas relações envolve diretamente a manipulação das propriedades das relações.

A palavra "relação" sugere muitas vezes exemplos familiares de relações, tais como, a relação de pai-para-filho, mãe-para-filho, irmão-para-irmã, etc. Exemplos similares também são freqüentemente encontrados na aritmética, onde temos relações como: "maior que", "menor que" ou "igual a". Também podemos dizer que existe uma relação entre a área de um círculo e seu raio, ou entre a área de um quadrado e seu lado. Estes exemplos sugerem relações entre dois objetos, no entanto, podemos citar relações entre três objetos, tais como a relação entre pai-mãe-filho, ou entre a área de um triângulo, sua base e sua altura. Exemplos similares também existem para relações entre quatro ou mais objetos.

Neste capítulo procuramos formalizar o conceito de relação e apresentamos métodos de representação, tais como matrizaes e grafos. As propriedades básicas são vistas e certas classes importantes de relações são introduzidas.

4.2 Definição de Relações

Pode-se definir relações como subconjunto próprio do produto cartesiano.

$$X_i \quad i = 1, ...n$$

onde n é o número de conjuntos. A relação definida no produto cartesiano:

$$\prod_{i=1}^{n} X_i \quad \mathcal{R} \subseteq \prod_{i=1}^{n} X_i$$

Com esta definição tem-se relações binária, ternária e n-ária.

Definição 4.2.1 *:* **Relação n-ária:** *Dados os conjuntos $X_1, X_2, ... X_n$, uma relação em $X_1 \, x \, X_2, ... X_n$ é um subconjunto de $X_1, X_2, ..., X_n$.*

Um caso especial de uma relação n-ária é a relação unária ρ em um conjunto X, a qual é apenas um subconjunto de X. Um elemento $x \in X$ satisfaz a relação se e somente se x pertencer ao subconjunto [7].

4.3 Relações Binárias

4.3.1 Definições

Na vida, as pessoas podem estabelecer várias relações. Um exemplo de relação binária é o que podemos chamar de conexão matrimonial (casamento). Neste caso, há um par "ordenado" (marido, mulher) que satisfaz a tal relação matrimonial. O ideal é que a relação entre seus elementos seja de um para um. O que às vezes nem sempre ocorre ... Em outro exemplo, duas pessoas podem ter também relação hierárquica (pai e filho). O análogo matemático considera as relações binárias para distinguir a ordem de pares de objetos de outros pares de objetos e seus relacionamentos.

Exemplo 4.3.1 *Se temos os conjuntos $X = \{1, 2\}$ e $Y = \{2, 3\}$, teremos que o produto cartesiano $X \, x \, Y = \{(1, 2), (1, 3), (2, 2), (2, 3)\}$. Se estamos interessados em distinguir elementos que são pares ordenados iguais $(x = y)$, escolheríamos o par $(2, 2)$ que satisfaz esta relação. Mas, se o interesse fosse aqueles cujo relacionamento é possuir um número menor do que o outro $(x < y)$, poderíamos escolher os pares $(1, 2)$, $(1, 3)$ e $(2, 3)$.*

Definição 4.3.1 *Dados dois conjuntos quaisquer X e Y, uma relação binária entre X e Y é um subconjunto obtido do produto cartesiano $X \times Y$ destes conjuntos. Uma relação binária é um subconjunto e é aqui denotada pela letra grega ρ (rho). Simbolicamente:*

$$x \, \rho \, y \longleftrightarrow (x, y) \in \rho$$

Observações:

- $\rho \subset X \times X$;
- a expressão $x\rho y$ equivale a dizer $(x, y) \in \rho$;
- o conjunto X é o conjunto de partida e o conjunto Y é o conjunto de chegada ou contradomínio;
- o número de relações binárias possíveis de X em Y é dado por $2^{n(X).n(Y)}$.

Exemplo 4.3.2 *Dados $X = \{1, 2\}$ e $Y = \{2, 3, 4\}$. A relação ρ é dada pela descrição $x \, \rho \, y \longleftrightarrow x + y$ é ímpar. Portanto, $(1, 2) \in \rho$, $(2, 3) \in \rho$ e $(1, 4) \in \rho$.*

Exercício 4.3.1 *Para cada uma das seguintes relações ρ em $\mathcal{N} \, x \, \mathcal{N}$, quais são os pares ordenados que pertencem a ρ:*

- $x \, \rho \, y \longleftrightarrow x = y + 1$; $(2, 2)(2, 3)(3, 3)(3, 2)$
- $x \, \rho \, y \longleftrightarrow x$ *divide* y; $(2, 4)(2, 5)(2, 6)$
- $x \, \rho \, y \longleftrightarrow x + y$ *é ímpar;* $(2, 3), (3, 4)(4, 5)(5, 6)$
- $x \, \rho \, y \longleftrightarrow x > y^2$; $(1, 2)(2, 1)(5, 2)(6, 4)(4, 3)$

A figura 4.1 mostra as quatro possibilidades de relacionamento entre os elementos dos conjuntos X e Y.

4.3.2 Domínio e Imagem de Relações

Definição 4.3.2 *Seja ρ uma relação binária. O conjunto $D(\rho)$ de todos os objetos x tais que para algum y, $(x, y) \in \rho$ é chamado de domínio de ρ, ou seja*

$$D(\rho) = \{x | \exists y((x, y) \in \rho)\}$$

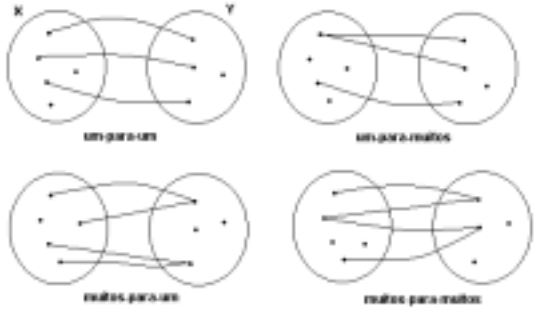

Figura 4.1: Tipos de relações binárias

Definição 4.3.3 *De maneira similar, o conjunto $R(\rho)$ de todos os objetos y tais que para algum x, $(x,y) \in \rho$ é chamado de imagem de ρ, ou seja*

$$R(\rho) = \{y | \exists x((x,y) \in \rho)\}$$

Em suma, dada uma relação $\rho = \{(x,y) \in X \times Y | x\rho y\}$, o conjunto dos valores de x chama-se domínio da relação e o conjunto dos valores de y chama-se de imagem da relação.

Sejam X e Y quaisquer dois conjuntos. Um subconjunto do produto cartesiano $X \times Y$ define uma relação ρ. Para qualquer relação ρ, temos que $D(\rho) \subseteq X$ e $R(\rho) \subseteq Y$ e a relação é dita uma relação "de X para Y". Se $Y = X$, então ρ é dita uma relação "de X para X" ou uma relaçãm "em X". Assim, qualquer relação em X é um subconjunto de $X \times X$ e é dita ser uma Relação Interna.

Uma operação foi definida como um conjunto de pares ordenados. Deste modo, é possível aplicar as operações usuais sobre conjuntos também sobre as relações. O conjunto resultante também será composto por pares ordenados e definirá uma relação.

Sejam R e S duas relações, então $R \cap S$ define uma relação tal que:

$$x(R \cap S)y = xRy \wedge xSy;$$

Do mesmo modo, $R \cup S$ define uma relação tal que:

$$x(R \cup S)y = xRy \vee xSy;$$

e também

$$x(R - S)y = xRy \wedge x \not S = (x,y) \in R \wedge (x,y) \notin S;$$

e finalmente

$$x(\sim R)y = x \not Ry = (x,y) \notin R.$$

4.4 Propriedades das Relações Binárias

Uma relação em um conjunto X tem certas propriedades.

4.4.1 Relação de Igualdade

A relação de igualdade num conjunto X, implica que o par (x, y) pertence a relação se $x = y$. Esta relação de igualdade tem três propriedades:

1. para qualquer $x \in X$, $x = x$, ou $(x, x) \in \rho$;
2. para qualquer x, $y \in X$, se $x = y$ portanto, $y = x$, ou $(x, y) \in \rho \rightarrow (y, x) \in \rho$;
3. para qualquer x, y, $z \in X$, se $x = y$ e $y = z$ ou $[(x, y)] \in \rho$ e $(y, z) \in \rho \rightarrow (x, z) \in \rho$.

Estas três propriedades fazem com que a relação de igualdade seja reflexiva, simétrica e transitiva.

4.4.2 Relação Reflexiva

Definição 4.4.1 *Uma relação binária ρ em um conjunto X é reflexiva se, para todo $x \in X$, $x\rho x$, ou seja*

$$(\forall x)(x \in X \rightarrow (x, x) \in \rho)$$

A relação $\leq$ é reflexiva no conjunto dos números reais uma vez que, para todo x,temos que $x \leq x$. Do mesmo modo, o relação de inclusão "contido ou igual" é reflexiva na família de todos os subconjuntos de um conjunto Universo. A relação de igualdade de conjuntos também é reflexiva. Por outro lado, a relação $<$ não é reflexiva no conjunto dos números reais, assim como a relação dos subconjuntos próprios na família dos subconjuntos de um conjunto Universo.

4.4.3 Relação Simétrica

Definição 4.4.2 *: Uma relação ρ em um conjunto X é simétrica se, para todo x e y em X:*

$$(x, y) \in \rho \rightarrow (y, x) \in \rho$$

As relações $\leq$ e $<$ não são simétricas no conjunto dos números reais, enquanto a relação de igualdade é. A relação de ser irmão não é simétrica no conjunto de todas as pessoas, mas é simétrica no conjunto dos homens.

4.4.4 Relação Transitiva

Definição 4.4.3 *: Uma relação ρ em um conjunto X é transitiva se, para todo x, y, e z em X:*

$$(x, y) \in \rho \wedge (y, z) \in \rho \rightarrow (x, z) \in \rho$$

As relações $\leq$, $<$ e $=$ são transitivas no conjunto dos números reais. As relações $\subseteq$, $\subset$ e de igualdade são também transitivas na família dos subconjuntos de um conjunto Universo. Entretanto a relação "ser mãe" não é transitiva.

4.4.5 Relação Anti-simétrica

Definição 4.4.4 *Uma relação ρ em um conjunto X é anti-simétrica se, para todo x e y em X:*

$$(x, y) \in \rho \wedge (y, x) \in \rho \rightarrow x = y$$

Repare que é possível possuir uma relação que seja ao mesmo tempo simétrica e anti-simétrica. Este é o caso onde cada elemento está relacionado consigo mesmo e não está relcionado com nenhum outro elemento.

Vejamos agora algumas relações conhecidas e suas propriedades:

Seja $\Re$ o conjunto dos números reais. As relações $>$ e $<$ em $\Re$ são transitivas. A relação de igualdade $=$ em $\Re$ é reflexiva, simétrica e transitiva.

Seja X o conjunto de todos as disciplinas oferecidas em uma universidade, e para $x \in X$ e $y \in X$, $x \rho y$ se x é um pré-requisito para y. Esta relação é transitiva.

Seja X o conjunto de todos os homens brasileiros e seja $x \rho y$ a relação x é irmão de y. Esta relação é simétrica.

Seja X o conjunto de todos os subconjuntos de um conjunto Universo. A relação de subconjunto em X é reflexiva, anti-simétrica e transitiva. Já a relação subconjunto próprio é apenas anti-simétrica e transitiva.

Classes importantes de relações que possuam uma ou mais destas propriedades serão vistas mais adiante neste capítulo.

4.5 Matrizes e Grafos Representando Relações

Uma relação ρ de um conjunto finito X para um conjunto finito Y pode ser representada através de uma matriz da relação ρ.

Sejam $X = \{x_1, x_2, ..., x_m\}, Y = \{y_1, y_2, ..., y_n\}$, e ρ uma relação de X em Y. A matriz da relação ρ pode ser obtida da seguinte maneira:

$$r_{ij} = \begin{cases} 1 & se\ x_i \rho y_j \\ 0 & se\ x_i \not\rho y_j \end{cases}$$

onde r_{ij} é o elemento da i-ésima linha e j-ésima coluna. Se X tem m elementos e Y tem n elementos, então a matriz da relação é uma matriz $m \times n$.

Considere como exemplo a relação $x\rho y$ de X em Y com $m = 3$ e $n = 2$:

$$\rho = \{(x_1, y_1), (x_2, y_1), (x_3, y_2), (x_2, y_2)\}$$

A matriz da relação é:

$$\rho = \begin{bmatrix} 1 & 0 \\ 1 & 1 \\ 0 & 1 \end{bmatrix} \tag{4.1}$$

A partir de agora e ao longo desta subseção, assumiremos que as relações são definidas em um conjunto X. Observando a matriz da relação podemos perceber algumas das propriedades de uma relação em um conjunto. Se a relação é reflexiva, então toda a diagonal da matriz deve ser 1. Se a relação é simétrica, então a matriz da relação também é simétrica. Se a relação for anti-simétrica, então a matriz é tal que se $r_{ij} = 1$, então $r_{ji} = 0$ para todo $i \neq j$.

Uma relação também pode ser representada graficamente através do desenho de seu *" grafo"*. Seja ρ uma relação em um conjunto $X = \{x_1, ..., x_m\}$. os elementos de X são representados por pontos ou círculos chamados *"nós"* ou *"vértices"*. Os nós correspondentes a x_i e x_j são identificados como x_i e x_j respectivamente. Se $x_i \rho x_j$, isto é, se $(x_i, x_j) \in \rho$, então conecta-se os nós x_i e x_j através de um arco e coloca-se uma seta no arco na direção de x_i para x_j. Quando todos os nós correspondentes aos pares ordenados da relação ρ estiverem conectados através de arcos orientados, tem-se então um grafo da relação ρ.

Através do grafo de uma relação é possível observar algumas das suas propriedades. Se uma relação for reflexiva, então deve existir um arco em ciclo, ou um "loop" para cada nó. Se uma relaão for simétrica, se existir um arco orientado conectando o nó x_i ao nó x_j, então deverá haver um outro arco orientado do nó x_j para o nó x_i. Para relações anti-simétricas, nenhum destes arcos-de-retorno deverão existir. Se uma relação for transitiva, a visualização desta propriedade através de grafos não é tão simples, de qualquer modo, os grafos da figura 4.3 ilustram algumas relações transitivas.

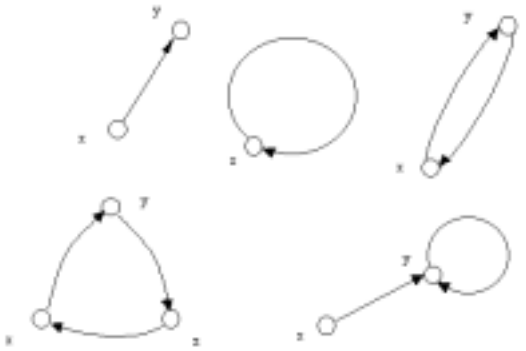

Figura 4.2: Grafos de diferentes tipos de relações binárias

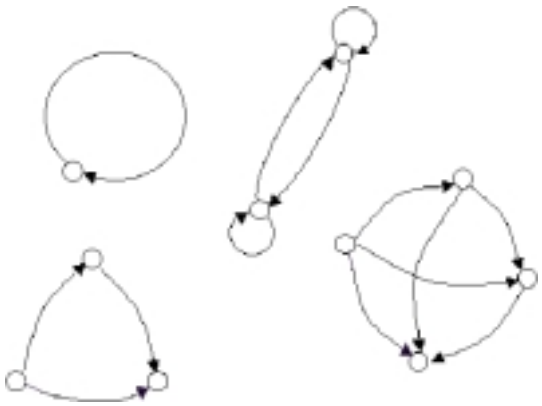

Figura 4.3: Grafos de relações transitivas

4.6 Partição e Cobertura de um Conjunto

Definição 4.6.1 *Seja S um dado conjuto e $A = \{A_1, A_2, ..., A_m\}$ onde cada A_i, $i = 1, ..., m$ é um subconjunto de S e*

$$\bigcup_{i=1}^{m} A_i = S$$

Então, o conjunto A é chamado de "cobertura" de S e os conjuntos $A_1, A_2, ..., A_m$ "cobrem" S. Se além disso, os elementos de A, que são subconjuntos de S forem mutuamente disjuntos,ou seja

$$\bigcap_{i=1}^{m} A_i = \emptyset$$

.

Figura 4.4: Grafos de relações simétricas e anti-simétricas

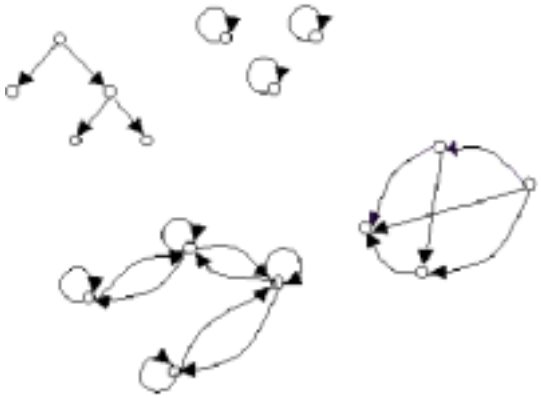

Figura 4.5: Grafos de relações binárias

Então A é chamado de "partição" de S e os conjuntos $A_1, A_2, ..., A_m$ são chamados de "blocos" da partição.

Exemplo 4.6.1 *Seja $S = \{a, b, c\}$ e consideremos os seguintes subconjuntos de S.*

$$A = \{\{a, b\}, \{b, c\}\ B = \{\{a\}, \{a, c\}\}\ C = \{\{a\}, \{b, c\}\}$$

$$D = \{\{a, b, c\}\}\ E = \{\{a\}, \{b\}, \{c\}\}\ F = \{\{a\}, \{a, b\}, \{a, c\}\}$$

os conjuntos A e F são coberturas de S enquanto que C,D e E são partições de S.

4.7 Relação de Equivalência

Definição 4.7.1 *Uma relação ρ em um conjunto X é uma relação de equivalência se:*

1. *ρ for reflexivo, isto é, para cada $x \in X$, $(x, x) \in \rho$*
2. *ρ for transitivo, isto é, $(x, y) \in \rho$ e $(y, z) \in \rho \rightarrow (x, z) \in \rho$*
3. *ρ for simétrico, isto é, $(x, y) \in \rho \rightarrow (y, x) \in \rho$*

Uma relação de equivalência é generalização da relação de igualdade [7]. Para cada elemento em um conjunto:

- $x = x$
- $x = y$ e $y = z$ implica que $x = z$
- $x = y$ implica em $y = x$

São exemplos de relações de equivalência:

1. A igualdade de números em um conjunto de números reais.
2. A igualdade de subconjuntos em um conjunto Universo.
3. A similaridade de triângulos em um conjunto de triângulos.
4. A relação entre linhas que são paralelas em um conjunto de linhas de um plano.
5. A relação de habitantes da mesma cidade no conjunto das pessoas que moram em Santa Catarina.
6. A relação de proposições que são equivalentes em um conjunto de proposições.

4.7.1 Classe de Equivalência

Uma relação de equivalência num conjunto divide-o em partições, colocando os elementos que são relacionados a cada um dos outros numa mesma classe, denominada de classe de equivalência. Estas classes de equivalência podem ser tratadas como entidades.

Exemplo 4.7.1 *A figura 4.6 mostra a partição do conjunto $\mathcal{N}$ em duas classes de equivalência.*

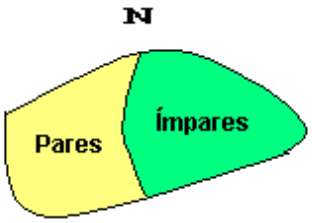

Figura 4.6: Partição de um conjunto em classes de equivalência

4.7.2 Exemplos

Exemplo 4.7.2 *Dois números inteiros são ditos equivalentes se o resto da divisão do número escolhido é o mesmo. Por exemplo, 10 dividido por 9 dá resto 1, isto é equivalente a 19 dividido por 9. Assim 10 é equivalente a 19, 28, 37, etc... por ter resto 1 quando divididos por 9.*

Exemplo 4.7.3 *Ser par ou ímpar. Todos os números pares estão em equivalência ao serem divididos por 2 darem resto 0. Assim como, todos os números ímpares estão em equivalência ao serem divididos por 2 darem resto 1.*

Exercício 4.7.1 *Dado o conjunto* $X = \{1, 2, 3, 4\}$ *e*
$\rho = \{(1,1), (1,4), (4,1), (4,4), (2,2), (2,3), (3,2), (3,3)\}$.
Escreva a matriz de ρ*, desenhe seu grafo e mostre que esta é uma relação de equivalência.*

Exercício 4.7.2 *Seja* $X = \{1, 2, ...7\}$ *e* $\rho = \{(x-y) \,|\, x - y$ *é divisível por 3*$\}$.
Mostre que ρ *é uma relação de equivalência e desenhe o grafo de* ρ.

Exercício 4.7.3 *Seja* $\mathcal{Z}$ *o conjunto dos inteiros e seja* ρ *a relação chamada "módulo congruente 3" definida por*

$\rho = \{(x,y) | x \in \mathcal{Z} \wedge y \in \mathcal{Z} \wedge (x-y)$ *é divisível por 3*$\}$.

Determine as classes de equivalência geradas pelos elementos de $\mathcal{Z}$.

4.8 Relação de Compatibilidade

Definição 4.8.1 *Uma relação* ρ *em* X *é chamada uma "relação de compatibilidade" se ela é reflexiva e simétrica.*

Exemplo 4.8.1 *Seja* $X = \{ball, bed, dog, egg, let\}$ *e seja* ρ *a relação dada por*

$\rho = \{(x, y) | x, y \in X \wedge x \rho y$ *se* x *e* y *possuem alguma letra em comum* $\}$.

Então ρ *é uma relação de compatibilidade e* x *e* y *são chamados compatíveis se* $x \rho y$.

Embora uma relação de equivalência em um conjunto defina uma partição de um conjunto em classes de equivalência, uma relação de compatibilidade não necessariamente define uma partição. Entretanto ela definie uma *cobertura* do conjunto.

4.9 Relação de Ordem

A relação de ordem é uma generalização do conceito de menor ou igual ($\leq$) ou de maior ou igual ($\geq$). Uma relação de ordem é reflexiva, antisimétrica e transitiva. A relação de ordem é interna e só existe se comparar elementos do mesmo conjunto.

4.9.1 Relação de Ordem Total

Se todos os elementos podem ser comparáveis esta relação é de ordem total.

Definição 4.9.1 *Uma relação de ordem* ρ *num conjunto não vazio* A *tal que todos os elementos de* A *são comparáveis dois a dois pela* ρ *chama-se relação de ordem total* ρ *em* A. *Portanto, uma relação de ordem total* ρ *em* A *é uma ordem que satisfaz a condição:*

$$(\forall x)(\forall y)(x, y \in A \ \ e \ \ x \rho y \ ou \ y \rho x)$$

Exemplo 4.9.1 *A ordem natural "*$x \leq y$*" no conjunto* $\mathcal{R}$ *dos números reais é uma ordem total em* $\Re$, *porque, quaisquer que sejam os números reais* x *e* y, *se tem* $x \leq y$ *ou* $y \leq x$, *isto é, dois números reais quaisquer são comparáveis pela ordem natural em* $\Re$.

Exemplo 4.9.2 *A relação no conjunto* $A = \{2, 4, 8, ... 2^n, ...\}$ *definida por "*x*" é um múltiplo de "*y*" é uma ordem total em* A, *porque dois elementos quaisquer de* A *são visivelmente comparáveis por esta ordem (cada elemento de* A *a partir do* 2^o *é múltiplo de cada um dos elementos que o precedem).*

4.9.2 Relação de Ordem Parcial

Se a relação é reflexiva, transitiva e anti-simétrica mas não é universal, ou seja, não vale para todos os elementos do conjunto considerado (alguns não são comparáveis)

é uma relação de ordem parcial. Os POSET (parcial order sets) são os conjuntos munidos de ordem parcial [5].

Exemplo 4.9.3 *A relação no conjunto $\mathcal{N}$ dos números naturais definida por "$x|y$" (relação de divisibilidade) é uma ordem parcial em $\mathcal{N}$, porque dois inteiros naturais nem sempre são comparáveis por esta ordem, como por exemplo, 5 e 7 (5 não divide 7 e 7 não divide 5).*

Observa-se que não tem sentido falar de ordem total ou parcial em relações de equivalência. Em relações $n-$árias também não tem sentido falar em ordem.

4.10 Relações Externas

Quanto aos conjuntos envolvidos, uma relação é dita *"externa"* se tomarmos os elementos de conjuntos distintos e verificarmos a relação entre estes elementos. Numa relação externa tem-se:

$$X_1 \neq X_2 \neq \ ... \ \neq X_n$$

Exemplo 4.10.1 *Dado um conjunto de cadeiras e um conjunto de pessoas, a relação pode ser definida pela maneira que as pessoas irão sentar-se nestas cadeiras. Como as pessoas são diferentes das cadeiras, esta relação é externa (entre conjuntos distintos.*

Na Computação, a grande aplicação das relações externas são os banco de dados que utilizam modelos relacionais. Os modelos relacionais são compostos de relações, ou tabelas bi-dimensionais, cujas operações são descritas em termos de álgebra relacional. Com este modelo, as tabelas de dados podem ser manipuladas para retornar outras tabelas de dados oferecendo aos usuários informações. Todas as estruturas de banco de dados relacionais são compostas por uma série de relações.

Exemplo 4.10.2 *Dados os seguintes conjuntos A de alunos, D de disciplinas oferecidas em um semestre no Curso de Computação e L dos locais (salas) onde serão ministradas as aulas:*

$A = \{Paulo, Carlos, Maria, Henrique\}$

$D = \{INE2135, INE3215, INE5371, INE2312\}$

$L = \{Alceu, Pequena, Reu1, Reu2\}$

$H = \{8-10, 10-12\}$

A relação entre os conjuntos alunos e disciplinas fornece a relação $R_1 = A \, x \, D$ conforme 4.1:

Paulo	*INE2135*
Paulo	*INE5371*
Carlos	*INE2312*
Maria	*INE5371*
Henrique	*INE3215*

Tabela 4.1: R_1 = Alunos x Disciplinas

A relação $R_2 = D\,x\,L$ fornece a relação entre as disciplinas e seus locais conforme 4.2.

INE2135	*Alceu*
INE3215	*Pequena*
INE5371	*Reu1*
INE2312	*Reu2*

Tabela 4.2: R_2 = Disciplinas x Locais

Uma relação $R_3 = L\,x\,H$ pode ser feita para resolver o problema de como alocar o local e o horário conforme 4.3.

Alceu	*8-10*
Alceu	*10-12*

Tabela 4.3: R_3 = Locais x Horários

As sub-relações de uma relação dada podem ser obtidas através de extração de propriedades que caracterizam a relação. Isto é feito por operações unárias de seleção e projeção. Por exemplo, ao se selecionar "Paulo" da R_1 cria-se uma nova sub-relação que indica quais os cursos o aluno Paulo irá fazer. Estas manipulações podem ser feitas no computador utilizando linguagens de base de dados como a SQL.

4.11 Composição de Relações Binárias

Como já foi visto, uma relação binária é um conjunto de pares ordenados. Deste modo, as operações usuais sobre conjuntos, tais como união, interseção, etc., quando aplicadas sobre as relações produzem outras relações.

Nesta seção examinaremos outro tipo de operação sobre as relações, ou seja, relações que são formadas em duas ou mais etapas. Exemplos da vida corrente deste tipo de operação são dados por casos como o de ser sobrinho, isto é, o filho do irmão ou da irmã; ou o de ser tio, que é o irmão do pai ou da mãe/ ou ainda o de ser avô, que é o pai do pai ou da mãe. Estas relações podem ser produzidas através da seguinte definição:

Definição 4.11.1 *Seja R a relação de X para Y e S a relação de Y para Z. Então a relação escrita como $R \circ S$ é chamada uma "relação composta" de R e S onde*

$$R \circ S = \{(x, z) | x \in X \wedge z \in Z \wedge \exists y (y \in Y \wedge (x, y) \in R \wedge (y, z) \in S)\}$$

A operação de obtenção de $R \circ S$ de R e S é chamada "composição" de relações.

Repare que $R \circ S$ é vazia se a interseção da imagem de R e do domínio de S for vazia. $R \circ S$ é não vazia se existir pelo menos um par ordenado $(x, y) \in R$ tal que o segundo membro $y \in Y$ do par ordenado o primeiro membro de um par ordenado em S.

Através dos grafos de R e de S, podemos realmente construir e visualizar o grafo de $R \circ S$, como pode ser visto na figura 4.7 abaixo.

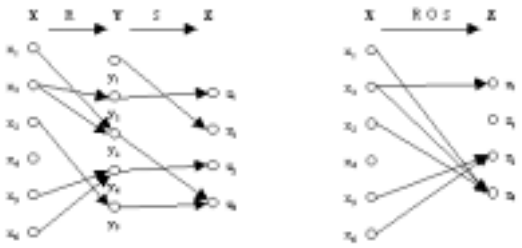

Figura 4.7: Relações R, S e a composta $R \circ S$

A operação de composição é uma operação binária sobre relações e portanto produz uma relação a partir de duas relações. As mesmas operações podem ser aplicadas novamente para produzir outras relações.

Não é difícil provar que a operação de composição sobre relações é associativa, isto é,

$$(R \circ S) \circ P = R \circ (S \circ P) = R \circ S \circ P$$

Exemplo 4.11.1 *Seja* $R = \{(1,2),(3,4),(2,2)\}$ *e* $S = \{(4,2),((2,5),(3,1),(1,3)\}$. *Ache* $R \circ S$, $S \circ R$, $R \circ (S \circ R)$, $(R \circ S) \circ R$, $R \circ R$, $S \circ S$ *e* $R \circ R \circ R$.

$$R \circ S = \{(1,5),(3,2),(2,5)\}$$

$$S \circ R = \{(4,2),(3,2),(1,4)\}$$

$$(R \circ S) \circ R = \{(3,2)\}$$

$$R \circ (S \circ R) = \{(3,2)\}$$

$$R \circ R = \{(1,2),(2,2)\}$$

$$S \circ S = \{(4,5),(3,3),(1,1)\}$$

$$R \circ R \circ R = \{(1,2),(2,2)\}$$

Exemplo 4.11.2 *Seja* R *e* S *duas relações sobre o conjunto dos inteiros positivos* $\mathcal{I}$.
$R = \{(x,2x)|x \in \mathcal{I}\}$ *e* $S = \{(x,7x)|x \in \mathcal{I}\}$
Ache $R \circ S$, $R \circ R$, $R \circ R \circ R$ *e* $R \circ S \circ R$.

$$R \circ S = \{(x,14x)|x \in \mathcal{I}\}$$

$$R \circ R = \{(x,4x)|x \in \mathcal{I}\}$$

$$R \circ R \circ R = \{(x,8x)|x \in \mathcal{I}\}$$

$$R \circ S \circ R = \{(x,28x)|x \in \mathcal{I}\}$$

A matriz da relação de uma relação R de um conjunto $X = \{x_1, x_2, ..., x_m\}$ para um conjunto $Y = \{y_1, y_2, ..., y_n\}$ é formada por uma matriz de dimensões $m \times n$ e chamada de M_R, cujos elementos são $1's$ e $0's$.

Do mesmo modo, chamamos de M_S a matriz da relação S de Y em $Z = \{z_1, z_2, ..., z_p\}$ cujas dimensóes são $n \times p$.

Para construir a matriz $M_{R \circ S}$, percorremos a $i^{ésima}$ linha de M_R e a $k^{ésima}$ coluna de M_S procurando ao menos um elemento j, tal que o elemento da posição j da linha, bem como da posição j da coluna percorrida seja 1. Então a posição $[i,k]$ de $M_{R \circ S}$ recebe 1, caso contrário recebe 0. Ou seja, a verredura de uma linha de M_R com cada coluna de M_S produz uma linha de $M_{R \circ S}$.

Exemplo 4.11.3 *Para as relações R e S dados no exemplo 4.11.1 sobre o conjunto [1,2,...,5], obter as matrizes das relações $R \circ S$ e $S \circ R$.*

$$M_R = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} \tag{4.2}$$

$$M_S = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} \tag{4.3}$$

$$M_{R \circ S} = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} \tag{4.4}$$

$$M_{S \circ R} = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} \tag{4.5}$$

Capítulo 5

Funções

5.1 Introdução

Neste capítulo estudaremos uma classe particular de relações chamadas de *funções*. Nos preocuparemos principalmente com funções chamadas *discretas*, que são aquelas que transformam um conjunto finito em outro conjunto finito. Existem diversas aplicações de funções dentro da área da Ciência da Computação. A saída gerada por um programa de computador pode ser considerada como uma função dos valores obtidos na entrada. Um compilador transforma um programa em um conjunto de instruções em linguagem de máquina. Uma classe especial de funções, conhecidas como funções de hashing, são funções utilizadas para organizar o armazenamento e acesso de dados em arquivos de computadores. Neste capítulo aborda-se também os conceitos de funções computáveis, parcialmente computáveis e não-computáveis. Aborda-se também o conceito de recursividade, de um computador abstrato e de máquina de Turing.

5.2 Conceito de Função

Definição 5.2.1 *Seja X e Y quaisquer dois conjuntos. A relação f de X para Y é chamada uma* função *se para todo $x \in X$ existe um único $y \in Y$ tal que $(x, y) \in f$, e se lê "f é função de X em Y"..*

$$f : X \to Y$$

Intuitivamente, função é uma relação especial entre dois conjuntos na qual todo elemento do primeiro conjunto deve ter, obrigatoriamente, elemento associado no

segundo conjunto e cada elemento do primeiro conjunto só pode ter um, e apenas um, elemento associado no segundo conjunto.

Voltando-se ao conceitos primeiros, retirando-se o conceito de pertence e criando-se o conceito de função teremos:

$$< U, X, x, f >$$

Assim temos que a função mapeia em um conjunto universo U num conjunto particular de dois elementos:

$$f : U \rightarrow x_1, x_2$$

Assim quando manda a U o elemento x_1 pertence ao conjunto pode-se ser representado por:

$$U \mapsto x_1 \in$$

E o mesmo pode ser dito para quando manda a U o elemento x_2 não pertence ao conjunto:

$$U \mapsto x_2 \notin$$

5.3 Domínio, Contradomínio e Imagem

Se X e Y são conjuntos de partida e de chegada, respectivamente, a função f de X em Y é representada por $f : X \rightarrow Y$ Por outro lado, se a variável x representar qualquer elemento de X e se a variável y representar qualquer elemento do conjunto Y pode-se usar as seguintes notações:

$$f : x \rightarrow f(x); \;\; f : x \rightarrow y; \;\; y = f(x)$$

O elemento y que corresponde a x de acordo com f chama-se **imagem** de x para o valor da função f para o elemento x e, se indica por $f(x)$ que se lê: "f de x".

O conjunto X constituído pelos elementos x é chamado **domínio** da função f e é representado por $D(f)$ na figura 5.1. O conjunto de chegada Y é chamado **contradomínio** conforme a figura 5.1. E finalmente o conjunto constituído pelos elementos y, imagens de x é chamado conjunto-imagem ou imagem da função representando-se por $Im(f)$ ou $f(X)$ como mostra a figura 5.1.

Os casos mostrados a seguir correspondem a algums exemplo de funções.

1. Seja $X = \{1, 5, P, Pedro\}$, $Y = \{2, 5, 7, q, Maria\}$, e $f = \{(1, 2), (5, 7), (P, q), (Pedro, q)\}$. Então, $D(f) = X$, $Im(f) = \{2, 7, q\}$, e $f(1) = 2$, $f(5) = 7$, $f(P) = q$, $f(Pedro) = q$.

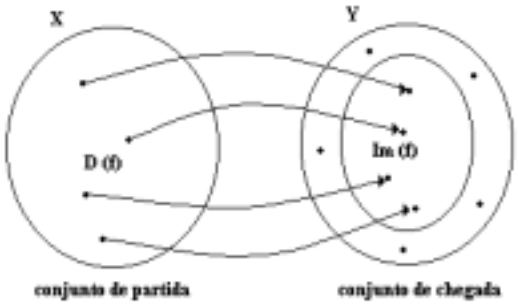

Figura 5.1: Domínio, Contradomínio e Imagem

2. Seja $X = Y = \Re$ e $f(x) = x^2 + 2$. Então, $D(f) = \Re$, $Im(f) \subseteq \Re$. Os valores de f para diferentes valores de $x \in \Re$ estão contidos em uma parábola.

3. Seja $X = Y = \Re$ e sejam

$$f = \{(x, x^2) | x \in \Re\}$$

$$f = \{(x^2, x) | x \in \Re\}$$

Obviamente f é uma função de X em Y. Entretanto, g não é uma função uma vez que a condição de unicidade é violada, isto é, para um mesmo valor de $x \in X$ vão corresponder dois valores de $y \in Y$.

4. Seja U o conjunto Universo e $P(U)$ seu conjunto Potência. Para quaisquer dois conjuntos A, $B \in P(U)$, as operações de união e interseção são funções de $P(U) \times P(U)$ em $P(U)$.

5. Seja P o conjunto de todos os inteiros positivos e $\sigma : P \to P$ seja tal que $\sigma(n) = n + 1$ onde $n \in P$. Assim, $\sigma(1) = 2, \sigma(2) = 3, ...$ A função σ é chamada *função sucessora de Peano* e é utilizada na descrição dos números inteiros.

Sabemos que nem todos os possíveis subconjuntos de $X \times Y$ constituem-se em funções de X em Y. O conjunto de todos os subconjunto de $X \times Y$ que definem uma função é denotado por Y^X. A razão da utilização desta notação fica clara através do exemplo a seguir.

Exemplo 5.3.1 *Seja* $X = \{a, b, c\}$ *e* $Y = \{0, 1\}$. *Então*

$$X \times Y = \{(a, 0), (b, 0), (c, 0), (a, 1), (b, 1), (c, 1)\}$$

e existem 2^6 subconjuntos possíveis de $X \times Y$. Destes, apenas 2^3 subconjuntos definem funções de X em Y.

$$f_0 = \{(a,0),(b,0),(c,0)\} \quad f_4 = \{(a,1),(b,0),(c,0)\}$$
$$f_1 = \{(a,0),(b,0),(c,1)\} \quad f_5 = \{(a,1),(b,0),(c,1)\}$$
$$f_2 = \{(a,0),(b,1),(c,0)\} \quad f_6 = \{(a,1),(b,1),(c,0)\}$$
$$f_3 = \{(a,0),(b,1),(c,1)\} \quad f_7 = \{(a,1),(b,1),(c,1)\}$$

5.4 Tipos de funções

5.4.1 Funções injetora, sobrejetora e bijetora

Função Injetora

Definição 5.4.1 *Uma função f de X em Y ($f : X \to Y$) é injetora se, elementos diferentes de X , têm imagens distintas em Y.*

$$\forall x_1 \in X, \forall x_2 \in X, (x_1 \neq x_2) \Rightarrow f(x_1) \neq f(x_2)$$

Função Sobrejetora

Definição 5.4.2 *Uma função f de X em Y ($f : X \to Y$) é sobrejetora se, todos os elementos de Y, são imagens dos elementos de X.*

$$\forall y \in Y, \exists x \in X | (x,y) \in f$$

Função Bijetora

Definição 5.4.3 *Uma função f de X em Y ($f : X \to Y$) é bijetora se, for injetora e sobrejetora ao mesmo tempo.*

Na letra **a** da figura 5.2 tem-se a função:

$$f : X \to Y = \{(1,a),(2,b),(3,c),(4,d)\}$$

A imagem é o conjunto ordenado $Im(f) = (a,b,c,d)$. Esta função possui elementos diferentes no domínio X que têm imagens distintas no contradomínio Y. Observa-se no diagrama, que nenhuma flecha que parte de X converge para um

mesmo elemento de Y, e que na representação da função, através do conjunto de pares ordenados, todos os segundos elementos dos pares são diferentes entre si. Além disso, a imagem $Im(f)$ é uma seqüência em que todos os elementos são diferentes. Quando isso acontece, a função é dita injetora e que tem-se uma injeção de X em Y.

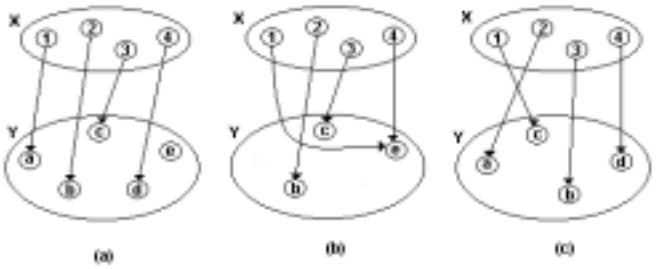

Figura 5.2: Funções injetora, sobrejetora e bijetora

Observando-se a letra **b** da figura 5.2 verifica-se que ao elemento "e" de X convergem duas flechas e que não existem elementos de Y que não recebem flechas, portanto, a função $f : X \to Y$ é sobrejetora pois o conjunto imagem é igual ao contradomínio, ou seja existe uma sobrejeção.

Na letra **c** da figura 5.2 a função $f : X \to Y = \{(1, c), (2, a), (3, b)(4, d)$ cuja imagem é o conjunto ordenado $Im(f) = (c, a, b, d)$. Nesta função todo elemento de Y é imagem de algum dos elementos de X. Isto significa que o conjunto que o conjunto imagem é igual ao contradomínio (sobrejeção) e que todos elementos do conjunto X tem imagens distintas no conjunto Y (injeção) então esta função é dita bijetora.

Exemplo 5.4.1 *Sendo S o conjunto de setores de um disco magnético rígido e C seu conjunto de cilindros. Pode-se definir uma função $a : S \to C$; onde $a(s)$ é o cilindro que contém o setor s. Naturalmente, cada cilindro é imagem a de setores que ele contém. Portanto, a é uma sobrejeção.*

Exercício 5.4.1 *Seja $\mathcal{N}$ o conjunto dos números naturais incluindo o zero. Determine quais das seguintes funções são injetoras, sobrejetoras e bijetoras.*

1. $f : \mathcal{N} \to \mathcal{N} \quad f(j) = j^2 + 2$
2. $f : \mathcal{N} \to \mathcal{N} \quad f(j) = j(mod\ 3)$

3. $f : \mathcal{N} \to \mathcal{N} \quad f(j) = \begin{cases} 1 & se\ j\ for\ impar \\ 0 & se\ j\ for\ par \end{cases}$

4. $f : \mathcal{N} \to \{0,1\} \quad f(j) = \begin{cases} 1 & se\ j\ for\ impar \\ 0 & se\ j\ for\ par \end{cases}$

Exercício 5.4.2 *Seja* $X = \{a,b,c\}$ *e* $Y = \{0,1\}$. *Liste todas as possíveis funções de* X *em* Y *e indique em cada caso se a função é injetora, sobrejetora ou bijetora.*

5.5 Função Composta

A operação de composição de relações pode ser estendida para as funções da seguinte maneira:

Dados os conjuntos X, Y e Z e as funções f de X em Y definida por $y = f(x)$ e g de Y em Z definida por $z = g(y)$, chama-se função composta de g com f a função $h = g \circ f$, de X em Z, definida por $z = g(f(x))$.

$$X \xrightarrow{f} Y \xrightarrow{g} Z$$

Deve ser observado que:

- Só existirá a função composta $g \circ f$ de X em Z se o contradomínio de f for um subconjunto do domínio de g.
- A composição de funções não é comutativa: $g \circ f \neq f \circ g$.

Exemplo 5.5.1 *Seja* $X = \{1,2,3\}$, $Y = \{p,q\}$ *e* $Z = \{a,b\}$. *Seja também* $f : X \to Y$ *dado por* $f = \{(1,p),(2,p),(3,q)\}$ *e* $g : Y \to Z$ *dado por* $f = \{(p,b),(q,b)\}$. *Ache* $g \circ f$.

$$g \circ f = \{(1,b),(2,b),(3,b)\}$$

.

Exemplo 5.5.2 *Seja* $X = \{1,2,3\}$ *e sejam* $f, g, h,$ *e* s, *funções de* X *em* X *definidas como*

$$f = \{(1,2),(2,3),(3,1)\} \quad g = \{(1,2),(2,1),(3,3)\}$$
$$h = \{(1,1),(2,2),(3,1)\} \quad s = \{(1,1),(2,2),(3,3)\}$$

Ache $f \circ g$; $g \circ f$; $f \circ h \circ g$; $s \circ g$; $g \circ s$; $s \circ s$; e $f \circ s$.

$$f \circ g = \{(1,3),(2,2),(3,1)\}$$

$$g \circ f = \{(1,1),(2,3),(3,2)\} \neq f \circ g$$

$$f \circ h \circ g = \{(1,3),(2,2),(3,2)\}$$

$$s \circ g = \{(1,2),(2,1),(3,3)\} = g = g \circ s$$

$$s \circ s = \{(1,1),(2,2),(3,3)\} = s$$

$$f \circ g = \{(1,2),(2,3),(3,1)\} = f$$

Exercício 5.5.1 *Seja $f(x) = x + 2$, $g(x) = x - 2$, e $h(x) = 3x$ para $x \in \Re$, onde $\Re$ é o conjunto dos números reais. Ache $g \circ f$; $f \circ g$; $f \circ f$; $g \circ g$; $f \circ h$; $h \circ g$;$h \circ f$; e $f \circ h \circ g$.*

$$g \circ f = \{(x,x) | x \in \Re\}$$

$$f \circ g = \{(x,x) | x \in \Re\}$$

$$f \circ f = \{(x,x+4) | x \in \Re\}$$

$$g \circ g = \{(x,x-4) | x \in \Re\}$$

$$f \circ h = \{(x,3x+2) | x \in \Re\}$$

$$h \circ g = \{(x,3x-6) | x \in \Re\}$$

$$h \circ f = \{(x,3x+6) | x \in \Re\}$$

$$f \circ h \circ g = \{(x,3x-4) | x \in \Re\}$$

Exercício 5.5.2 *Seja $f : \Re \to \Re$ e $g : \Re \to \Re$, onde $\Re$ é o conjunto dos números reais. Ache $f \circ g$ e $g \circ f$, onde $f(x) = x^2 - 2$ e $g(x) = x + 4$. Diga se estas funções são injetoras, sobrejetoras ou bijetoras.*

5.6 Função Inversa

Podemos facilmente verificar que o inverso de uma relação R de X para Y pode ser definida como a relação $\tilde{R}$ de Y para X tal que $(y,x) \in \tilde{R} \leftrightarrow (x,y) \in \mathrm{R}$; ou seja, os pares ordenados de $\tilde{R}$ são obtidos a partir de R simplesmente invertendo-se os membros dos pares ordenados. A situação não é exatamente a mesma para o caso das funções. Seja $\tilde{f}$ a inversa de f, onde f é considerada uma relação de $X \to Y$. $\tilde{f}$ pode não ser uma função, primeiramente por que o domínio de $\tilde{f}$ pode não ser Y, mas apenas um subconjunto de Y, e depois, $\tilde{f}$ pode ferir a condição de unicidade da definição de função.

Exemplo 5.6.1 *Seja* $X = \{1,2,3\}$ *e* $Y = \{p,q,r\}$, *e* $f : X \to Y$ *dada por* $f = \{(1,p),(2,q),(3,q)\}$. *Então* $\tilde{f} = \{(p,1),(q,2),(q,3)\}$ *não é uma função.*

Exemplo 5.6.2 *Seja* $\Re$ *o conjunto dos números reais e seja* $f : \Re \to \Re$ *dado por* $f = \{(x,x^2) | x \in \Re\}$.

Então $\tilde{f} = \{(x^2,x) | x \in \Re\}$ *não é uma função.*

Exemplo 5.6.3 *Seja* $X = \{0,1\}$ *e* $Y = \{p,q,r,s\}$, *e* $f : X \to Y$ *dada por* $f = \{(0,p),(1,r)\}$. *Então* $\tilde{f} = \{(p,0),(r,1)\}$ *é uma função de um subconjunto de* Y *em* X, *ou seja,* $\tilde{f} : \{p,r\} \to \{0,1\}$.

Pelos exemplos vistos acima, para uma dada $f : X \to Y$, $\tilde{f}$ è uma função somente se f for injetora. Entretanto, isto não garante que $\tilde{f}$ seja uma função de Y em X, mas apenas de um subconjuto de Y em X.

Duas funções dizem-se inversas uma da outra, quando o domínio da primeira é o contradomínio da segunda e, o contradomínio da primeira é o domínio da segunda. Portanto, se f é uma função de X em Y, a função inversa de f, $\tilde{f}$, agora designada por f^{-1} é:

$$f^{-1} : Y \to X$$

Deve ser observado que só pode existir f^{-1} inversa de f se ela for bijetora. Se f^{-1} existe, então f é chamada invertível. Obviamente, f^{-1} também é bijetora.

Exemplo 5.6.4 *Conhecendo-se o conjunto constituído pelos pares ordenados da função* f, *obtemos os pares ordenados da função inversa* f^{-1}, *trocando-se a posição dos elementos de cada par da função* f.

Se

$$f = \{(1,3),(2,6)(3,9)\}$$

então

$$f^{-1} = \{(3,1),(6,2)(9,3)\}$$

Seja a função $f : A \to B$ que é bijetora. A função inversa existe e é $f^{-1} : B \to A$ como mostrado no diagrama 5.3. Todavia, no diagrama 5.4 a função inversa não existe porque f não é bijetora (os elementos a e c possuem a mesma imagem y).

Definição 5.6.1 *Uma função* $I_x : X \to X$ *é chamada de* função identidade *se* $I_x = \{(x, x)|x \in X\}$.

Observe que para qualquer função $f : X \to X$, as funções $I_x \circ f$ e $f \circ I_x$ são ambas iguais a f. Estas propriedades da função identidade podem ser utilizadas para estabelecer o seguinte teorema sobre o inverso de uma função.

Teorema 5.6.1 *Se* $f : X \to X$ *possui função inversa, então*

$$f^{-1} \circ f = I_x \text{ e } f \circ f^{-1} = I_x$$

Exemplo 5.6.5 *Mostre que as funções* $f(x) = x^3$ *e* $g(x) = x^{1/3}$ *para* $x \in \Re$ *são inversas uma da outra.*

Uma vez que $(f \circ g)(x) = f(x^{1/3}) = x = I_x$ *e* $(g \circ f)(x) = f(x^3) = x = I_x$, *então* $f = g^{-1}$ *ou* $g = f^{-1}$.

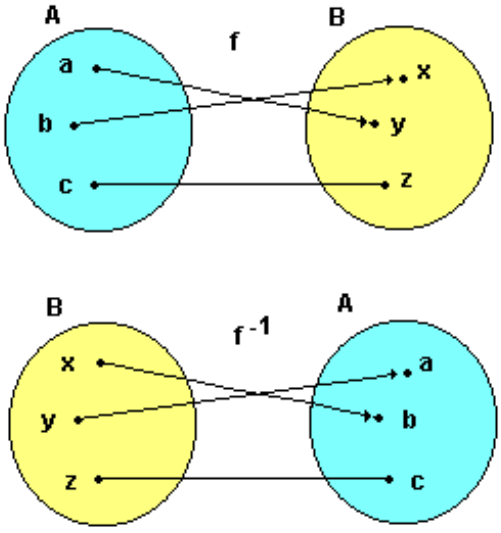

Figura 5.3: Função que tem inversa

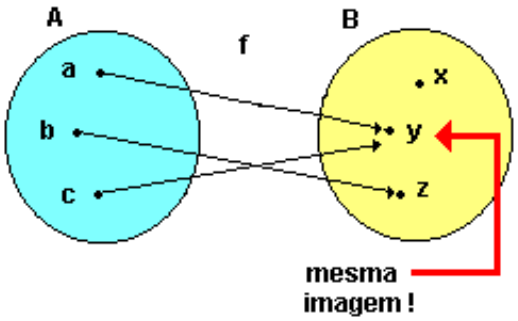

Figura 5.4: Função que não tem inversa

Exemplo 5.6.6 *Num esquema de criptografia, um transmissor (pessoa que envia a mensagem) deseja que esta chegue com segurança a seu receptor. O transmissor escreve a mensagem (em texto ao claro) e aplica um método de codificação para produzir uma mensagem cifrada. A mensagem codificada é então transmitida ao receptor que aplica um método de decodificação para converter o texto cifrado novamente em texto claro.*

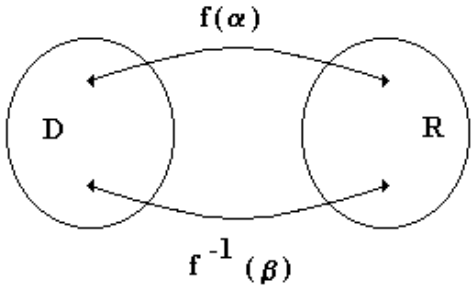

Figura 5.5: Esquema de Criptografia

Conforme a figura 5.5 tem-se D o domínio de mensagens não cifradas, e R o domínio de mensagens criptografadas.

A criptografia é a transformação do texto do domínio D para o domínio R aplicando uma função bijetora de tal modo que se possa calcular sua inversa. A função f deve ter um certo número de parâmetros $f(\alpha)$ e sua inversa f^{-1} tem um certo número de conjuntos β que será conhecido. Os parâmetros α é o que se chama a chave de codificação e os parâmetros β é a chave de decodificação. Desde que

conhecido $f(\alpha)$ calcula-se a $f^{-1}(\beta)$. Sabendo-se a chave β é possível ler o texto. O indivíduo que não saiba quem é o β não poderá ler o texto. Todavia, várias técnicas heurísticas de Inteligência Artificial podem ser utilizadas para descobrir β e quebrar o sigilo da mensagem, uma delas é a transposição de bits de um alfabeto. Uma maneira de dificultar esta quebra é não utilizar a transposição de letras para codificação. Outra maneira seria representar a função como uma seqüência de 0 e 1, pois assim teria-se 2^n possibilidades para se explorar com n bits. Atualmente, sistemas bancários utilizam chaves de 64 bits e colocar um computador para examinar todas as possibilidades poderia levar anos. Pode-se dizer que dada uma função, implementar sua inversa tem dificuldades diferentes. Geralmente, o que interessa é a computabilidade prática ou seja, resolver o problema em tempo hábil.

5.7 Função Característica de um Conjunto

Nesta seção veremos mais detalhadamente funções que mapeiam do conjunto Universo U para o conjunto $\{0, 1\}$. Uma correspondência de um-para-um é estabelecida entre estas funções e os conjuntos. Através da utliização destas funções, proposições sobre conjuntos e suas operações podem ser representadas em um computador através de números binários, de modo a facilitar a sua manipulação.

Definição 5.7.1 *Seja U um conjunto Universo e seja A um subconjunto de U. A função $\psi_A : U \to \{0,1\}$ definida como*

$$\psi_A(x) = \begin{cases} 1 & se\ x \in A \\ 0 & se\ x \notin A \end{cases}$$

é chamada de função característica *do conjunto A.*

Exemplo 5.7.1 *Seja U o conjunto de todas as pessoas moradoras em Florianópolis e seja M o conjunto das mulheres que mora em Florianópolis. Assim, ψ_F associa o número 1 com cada mulher e o número 0 com cada homem que more em Florianópolis.*

As propriedades a seguir sugere como podemos relacionar as funções características de conjuntos com as operações sobre conjuntos.

Seja A e B quaisquer 2 subconjuntos de um conjunto Universo U. Então as seguintes afirmações podem ser provadas para todo $x \in U$.

$$(1) \quad \psi_A(x) = 0 \leftrightarrow A = \emptyset$$

$$(2) \quad \psi_A(x) = 1 \leftrightarrow A = U$$

$$(3) \quad \psi_A(x) \leq \psi_B(x) \leftrightarrow A \subseteq B$$

$$(4) \quad \psi_A(x) = \psi_B(x) \leftrightarrow A = B$$

$$(5) \quad \psi_{A \cap B}(x) = \psi_A(x) * \psi_B(x)$$

$$(6) \quad \psi_{A \cup B}(x) = \psi_A(x) \pm \psi_B(x) - \psi_{A \cap B}(x)$$

$$(7) \quad \psi_{A \sim A}(x) = 1 - \psi_A(x)$$

$$(8) \quad \psi_{A-B}(x) = \psi_{A \cap \sim B}(x) = \psi_A(x) - \psi_{A \cap B}(x)$$

Repare que as operações $\leq$, $=$, $\pm$, e $-$ utilizadas com as funções características são as operações aritméticas usuais, uma vez que os valores das funções características são sempre 0 ou 1.

As propriedades acima podem ser facilmente provadas utilizando a definição de função característica. Por exemplo, a afirmação (5) acima pode ser provada da seguinte maneira:

$x \in A \cap B \leftrightarrow x \in A \wedge x \in B$, e por conseqüência $\psi_A(x) = 1$ e $\psi_B(x) = 1$ e $\psi_{A \cap B}(x) = 1 * 1 = 1$. Se $x \notin A \cap B$, então $\psi_A(x) = 0$ ou $\psi_B(x) = 1$ e portanto $\psi_{A \cap B}(x) = 0$.

5.8 Funções de Hash

Os conceitos de "arquivos", "registros", "campos", "chaves de busca", etc., são frequentemente utilizados quando se discute o armazenamento e recuperação de informações em computadores. Geralmente, as informações são armazendas em arquivos através de registros, e muitas vezes, os registros contêm um campo denominado de "chave". A chave possui um valor que identifica de maneira unívoca um registro dentro de um arquivo e portanto, pode ser também utilizada como uma indicação da posição do registro dentro do arquivo. Em um arquivo que contenha, por exemplo, o registro do histórico escolar de estudantes de uma universidade, o campo que representa o número de matrícula de cada estudante pode ser encarado como a chave do registro de contém o histórico de cada estudante.

Na organização direta de arquivos para acesso aleatório, o endereço de armazenamento do registro dentro do arquivo pode ser obtido reallizando-se alguma operação aritmética ou lógica sobre a representação interna da chave do registro. Qualquer tranformação que mapeie o valor do conjunto de chaves dos registros de um arquivo em um conjunto de endereços ou posições onde os registros estarão armazenados é chamada de *função de hash*.

Existem várias alternativas para funções de hash, uma das mais populares é chamada de "método da divisão" e será apresentada a seguir.

Antes de descrever a função de hash obtida através do método da divisão, observe que toda chave possui uma representação binária, a qual pode ser considerada como um número binário. Chamemos este valor numérico da chave de "k" e seja "n" um inteiro fixo (preferencialmente primo) adequadamente escolhido. Então a função de hash h obtida pelo método da divisão é

$$h(k) = k \ (mod n)$$

ou seja, $h(k)$ é o resto da divisão de k por n e portanto um elemento do conjunto $\{0, 1, 2, ...n-1\}$. Deste modo, esta função de hash mapeia o conjunto de chaves no conjunto de endereços $\{0, 1, 2, ...n-1\}$. A escolha de n depende do fato de que uma boa função de hash deve distribuir uniformemente os registros entre os elementos do conjunto de endereços.

Uma função de hash muitas vezes mapeia diferentes chaves para um mesmo elemento do conjunto de endereços. Assim, o conjunto de registro é particionado em n classes de equivalência. Torna-se necessário então, um mecanismo que realize o armazenamento e faça a recuperação de registros que eventualmente "colidam" em um mesmo endereço. Existem muitas técnicas, chamadas "técnicas para resoluação de colisões" que podem ser utilizadas para este propósito.

5.9 Recursividade

A Teoria da Computação, entre outras coisas, procura estudar os modelos matemáticos de dispositivos computacionais (ou máquinas) e os tipos de problemas que podem ser resolvidos por cada tipo de máquina. Dado um determinado problema, o procedimento padrão para determinar se este problema é 'computável', é reduzir o problema a um problema equivalente que consiste de uma função sobre os números naturais e então decidir seesta função pode ser resolvida pelo modelo do computador.

Nesta seção definiremos indutivamente uma classe de funções e mostraremos que estas funções podem ser resolvidas "mecanicamente". Esta classe de funções são chamadas *funções recursivas*, e nos resringiremos apenas àquelas funções cujos argumentos e valores são números naturais.

5.9.1 Funções Recursivas

Por generalização consideraremos funções de n variáveis denotadas com $f(x_1, x_2, ..., x_n)$. Se a função f for $f : \mathcal{N}^n \rightarrow \mathcal{N}$ ela é chamada "total", pois é definida para toda n-úpla em $\mathcal{N}^n$. por outro lado, se a função f for $f : D \rightarrow \mathcal{N}$ onde $Dsubseteq\mathcal{N}^n$, então f é chamada "parcial". Exemplos de tais funções são:

1. $f(x, y) = x + y$, a qual é definida para todo $x, y \in \mathcal{N}$ e portanto é uma função total.

2. $g(x, y) = x - y$, a qual é definida apenas para aqueles $x, y \in \mathcal{N}$ que satisfaçam $x \geq y$ e portanto é uma função parcial.

Veremos agora um conjunto de três funções chamadas *funções iniciais*, que são utilizadas para definir outras funções por indução.

$Z : Z(x) = 0$ - Função Zero

$S : S(x) = x + 1$ - Função Sucessor

$U_i^n : U_i^n(x_1, x_2, ..., x_n) = x_i$ - Função Projeção

A Função Projeção é também chamada de "função identidade generalizada". Como exemplos temos: $U_1{}^1(x) = x$, $U_2{}^2(x, y) = y$, $U_2{}^3(2, 4, 6) = 4$, etc...

A operação de composição será utilizada para gerar outras funções. Já vimos como funciona a composição de funções para uma variável. A mesma idéia pode ser utilizada para funções de mais de uma variável. Tomemos como exemplo o seguinte caso:

Sejam $f_1(x, y)$, $f_2(x, y)$, *e* $g(x, y)$ quaisquer três funções. A composição de g com f_1 e f_2 é uma função h dado por:

$$h(x, y) = g(f_1(x, y), f_2(x, y))$$

Se f_1, f_2 e g são funções totais, então h também é total. Generalizando, sejam $f_1, f_2, ..., f_n$ funções parciais de m variáveis e seja g uma função parcial de n variáveis. Então a composição de g com $f_1, f_2, ..., f_n$ produz uma função parcial h dada por:

$$h(x_1, ...x_n) = g(f_1(x_1, ..., x_m), ..., f_n(x_1, ...x_m))$$

Exemplo 5.9.1 *Sejam* $f_1(x, y) = x + y$, $f_2(x, y) = xy + y^2$, *e* $g(x, y) = xy$

$h(x, y) = g(f_1(x, y), f_2(x, y))$

$h(x, y) = g(x + y, xy + y^2)$

$h(x, y) = (x + y).(xy + y^2)$

Dada uma função $f(x_1, x_2, ..., x_n)$ de n variáveis, muitas vezes é conveniente considerar $n-1$ destas variáveis como fixas e variar apenas a variável restante sobre o domínio do números naturais ou sobre um subconjunto deste. Por exemplo, podemos tratar x como um parâmetro fixo e variar y em $f(x,y)$ para obter $f(x,0), f(x,1), f(x,2)$, etc. Apesar de parecer extremamente trabalhoso num processo de cálculo manual, esta técnica pode ser bastante interessante em um processo de computação automática. Vejamos, por exemplo, o cálculo de $f(2,3)$ onde $f(x,y) = x + y$. Assumimos que $f(2,0) = 2$, seja um valor dado e então prosseguimos calculando $f(2,1)$, $f(2,2)$, e finalmente $f(2,3)$. Cada valor da função (exceto $f(2,0)$) é calculado através da adição de 1 ao valor anterior da função até que o resultado desejado seja obtido. O cálculo de $f(2,3)$ fica então:

$f(2,3) = [(f(2,0)+1)+1]+1 =$

$f(2,3) = [(2+1)+1]+1 =$

$f(2,3) = [3+1]+1 = 4+1 = 5$

Assume-se que possuamos um mecanismo pelo qual possamos determinar o valor da função quando um argumento for zero, bem como seu valor para o argumento $n+1$ através do valor da função quando o argumento for n.

Recursão é a operação que define uma função $f(x-1, x_2, ..., x_n, y)$ de $n+1$ variáveis através do uso de outras duas funções $g(x_1, x_2, ..., x_n)$ e $h(x_1, x_2, ..., x_n, y, z)$ de n e $n+2$ variáveis respectivamente.

Nesta definição assume-se a variável y como sendo uma variável indutiva, no sentido de que o valor de f para $y+1$ pode ser expressa em termos de f para y. As variáveis $x_1, x_2, ..., x_n$ são tratadas como parâmetros fixos. Também assume-se g e h como funções conhecidas.

$$f(x_1, x_2, ..., x_n, 0) = g(x_1, x_2, ..., x_n)$$

$$f(x_1, x_2, ..., x_n, y+1) = h(x_1, x_2, ..., x_n, y, f(x_1, x_2, ..., x_n, y))$$

Definição 5.9.1 *Uma função f é chamada* primitiva recursiva *se e somente se ela puder ser obtida de funções iniciais através de um número finito de operações de composição e recursão.*

Exemplo 5.9.2 *Mostre que a função $f(x,y) = x + y$ é primitiva recursiva.*

Observe que $x + (y+1) = (x+y) + 1$, então

$f(x, y+1) = f(x,y) + 1 = S(f(x,y))$

também

$f(x,0) = x$

Podemos agora definir $f(x,y)$ *como*

$$f(x,0) \;=\; x \;=\; {U_1}^1(x)$$

$$f(x,y+1) \;=\; S({U_3}^3(x,y,f(x,y))$$

Aqui a função base é $g(x) = {U_1}^1(x)$ *e a função passo-indutiva é* $h(x,y,z) = S({U_3}^3(x,y,z))$.

Vejamos agora como calcular o valor de $f(2,4)$

$f(2,0) = 2$

$f(2,4) = S(f(2,3)) = S(S(f(2,2)))$

$= S(S(S(f(2,1)))) = S(S(S(S(f(2,0)))))$

$= S(S(S(S(2)))) = S(S(S(3))) = S(S(4)) = S(5) = 6.$

Exemplo 5.9.3 *Usando recursão, defina a função de multiplicação* $*$ *dada por*

$$g(x,y) = x * y$$

Uma vez que $g(x,0) = 0$ *e* $g(x,y+1) = g(x,y) + x$,

$g(x,0) = Z(x)$

$g(x,y+1) = f({U_3}^3(x,y,g(x,y)), {U_1}^3(x,y,g(x,y)))$

onde f *e a função de adição dada no exemplo anterior.*

É importante ressaltar que não é necessário utilizar apenas as funções iniciais na construcão de uma função primitiva recursiva. Se possuirmos um conjunto de funções $f_1, f_2, ..., f_n$ que são primitivas recursivas, então podemos utlizar quaisquer destas funções juntamente com as funções iniciais para obter outra função primitiva recursiva, desde que nos restrinjamos apenas às operações de composição e recursão.

As funções mostradas a seguir são funções primitivas recursivas freqüentemente utilizadas para construção de outras funções primitivas recursivas.

1. Função sinal, sg:

   $sg(0) = 0 \quad sg(y+1) = 1$
   ou $sg(0) = Z(0) \quad sg(y+1) = S(Z({U_2}^2(y, sg(y))))$

2. Função testa zero, $\widetilde{sg}$:

   $\widetilde{sg}(0) = 1 \quad \widetilde{sg}(y+1) = 0$
   ou $\widetilde{sg}(0) = S(0) \quad \widetilde{sg}(y+1) = Z({U_2}^2(y, \widetilde{sg}(y)))$

3. Função antecessor, A:

   $A(0) = 0 \quad A(y+1) = y = {U_1}^2(y, A(y))$

4. Função subtração própria, $\dot{-}$:

   $x\dot{-}0 = x \quad x\dot{-}(y+1) = A(x\dot{-}y)$

5. Função mínimo(x,y), $min(x,y) = x\dot{-}(x\dot{-}y)$

6. Função máximo(x,y), $max(x,y) = y + (x\dot{-}y)$

7. Função quadrática, $f(y) = y^2$:

   $f(y) = y^2 = U_1{}^1(y) * U_1{}^1(y)$

Exercício 5.9.1 *Mostre que a função $Pr(x)$ que calcula a paridade de um número é primitiva recursiva.*
Note que $Pr(0) = 0, \ \ Pr(1) = 1, \ \ Pr(2) = 0, \ \ Pr(3) = 1, \ \ ...$

Exercício 5.9.2 *Motre que a função Fatorial de um número (x!) é primitiva recursiva.*
Note que $0! = 1, \ \ 1! = 0! * 1, \ \ 2! = 1! * 2, \ \ ...$

Conforme já vimos anteriormente, um conjunto pode ser definido por meio de um predicado segundo o *princípio da especificação*, que atesta que todo predicado especifica um conjunto que é um subconjunto do conjunto Universo. Este subconjunto especificado pelo predicado é chamado de *extensão* do predicado sobre o conjunto Universo. Por exemplo, se $P(x)$ é um predicado, então o conjunto A é chamado extensão de $P(x)$ se $A = \{x|P(x)\}$.

Um predicado é primitivo recursivo se e somente se sua extensão for primitiva recursiva, ou seja, se a função característica que define um conjunto, extensão de um predicado P, for primitiva recursiva, então também o predicado é primitivo recursivo.

Por exemplo, os predicados "é primo" e "é divisor de n" são recursivos por que as funções características que mapeiam elementos do conjunto Universo no subconjunto $\{0,1\}$, indicando se o elemento pertence ou não pertence ao conjunto, são funções recursivas.

Exemplo 5.9.4 *Mostre que o predicado "x é primo" é primitivo recursivo.*

Um número x é um primo se e somente se ele possuir apenas dois divisores, 1 e x, desde que este número não seja nem 1 nem 0. Começamos calculando a função característica da extensão de "x não é primo" que e:

$$\psi_{Pr}(x) = sg(D(x)\dot{-}2) + \widetilde{sg}(|x-1|) + \widetilde{sg}(|x-0|)$$

onde $D(x)$ significa a função "número de divisores de x" que também é primitiva recursiva.

Se $\psi_{Pr}(x)$ é primitiva recursiva, então também a função característica $\psi_{Pr}(x)$ dado por $1\dot{-}\psi_{Pr}(x)$ é primitiva recursiva.

5.9.2 Recursividade em Linguagens de Programação

Ao longo da seção anterior definimos um conjutno de funções recursivas. A idéia básica é definir uma função para todos os seus valores de argumentos de uma forma construtiva, através da utlização da indução. O valor de uma função para um determinado valor de argumento pode ser calculado de forma recursiva, em um número finito de passos. Correspondendo a um passo recursivo na definição de uma função, algumas linguagens de programação disponibilizam rotinas ou sub-rotinas que podem conter chamadas para qualquer rotina, inclusive para si mesma. Uma rotina que contém chamadas para si mesma ou para uma segunda rotina que por sua vez chama a primeira rotina, é conhecida como uma rotina recursiva.

O programa a seguir em PASCAL contém uma rotina recursiva para cálculo do fatorial de um número.

```
program fat;

var
    n : integer;
function fatorial (n : integer) : integer;
begin
    if n = 0 then
      fatorial := 1
    else
      fatorial := fatorial(n);
end;

begin

    writeln('Entre o o numero a ser calculado o fatorial');
    readln(n);
    writeln('Fatorial = ',fatorial(n));
end.
```

5.10 Computabilidade de Funções

5.10.1 Funções computáveis

Já mostramos anteriormente que um conjunto é recursivo se e somente se a função característica que define o conjunto for primitiva recursiva, já que é a função característica é que determina se um determinado elemento x é ou não membro de um conjunto dado. Este processo de determinação se um determinado elemento é ou não membro de um conjunto é chamado de um *problema de decisão*. É altamente desejável saber antecipadamente se um determinado problema de decisão pode ser ou não resolvido por um computador (ser computável). De modo teórico, podemos dizer um problema é computável se a função característica do conjunto for recursiva.

De modo prático, dizemos que uma função é dita computável se para qualquer entrada de dados pode ser implementada no computador em tempo finito, ou seja, o programa irá parar para qualquer entrada de dados. A maioria das linguagens de programação oferecem algumas funções intrínsecas e também permitem aos programadores definir novas funções.

Exemplo 5.10.1 *Se queremos usar uma função que computa a média entre valores de três números reais podemos utilizar o seguinte código em PASCAL que permite definir tal função.*

function *media(x,y,z:real):real;*

{ *encontra a média dos valores de três números reais* }

begin { *função media* }

media : = (x + y + z) / 3.0;

end;

O cabeçalho **function** *dentro dos parênteses indica que a função consiste de todas 3-túplas de números reais. Para cada uma delas é esperado que a função produza um resultado único.*

5.10.2 Funções parcialmente computáveis

Supondo que estejamos interessados em gerar ou enumerar elementos de um conjunto cujos membros sejam inteiros. Podemos considerar este processo de geração como a geração dos elementos de uma função. Um conjunto é dito ser *recursivamente enumerável* se ele puder ser gerado por uma função recursiva. Dado um elemento

z que pertença a um conjunto, através de um tempo finito de cálculos da função recursiva, z será gerado e poderemos dizer que z pertence ao conjunto. Por outro lado, se z não pertencer ao conjunto e z não puder ser gerado em um tempo finito de computação, temos então um problema de semi-decisão associado ao conjunto. Podemos afirmar com certeza se o elemento pertence ao conjunto, mas não podemos ter certeza de que ele não pertece ao conjunto.

Exemplo 5.10.2 *Considere o conjunto de todos os divisores de um número, exceto o próprio número. Um número perfeito é aquele no qual a soma de todos os seus divisores é igual ao próprio número. O número 6, por exemplo, é um número perfeito, uma vez que* $1 + 2 + 3 = 6$. *Entretanto, não sabemos se a quantidade de números perfeitos é finita ou infinita.*

Suponhamos então um algoritmo que decida se existe um número perfeito maior que um dado número i. Este algoritmo é um exemplo de uma função parcialmente computável ou semi-computável, já que ele pode dizer **sim**, *se achar dentro de um tempo "finito" um número perfeito maior do que i, mas não pode dizer* **não**, *porque não sabemos se este conjunto é finito ou infinito.*

Em termos práticos, em computação, algumas funções não são definidas para algumas entradas. É impossível, dado um programa e sem conhecer sua estrutura interna garantir que ele termine com um certo tipo de entrada. Pode ocorrrer que se escolha um conjunto de dados de entrada e se o programa tiver laços pode entrar num laço infinito e nunca parar. Os programas podem gerar funções parcialmente computáveis.

Exemplo 5.10.3 *Considere a seguinte função em PASCAL:*

```
function f(x:integer):integer;
    var y:integer;
    begin
    y : = 1;
        while (x <> 0) do
            begin
            x:= x - 2;
            y:= y * 2
            end;
```

$f := y$
end;

Nota-se que a chamada $f(2k)$, com $k \geq 0$, retorna o número 2^k. Para qualquer outra entrada, o programa não pára. Portanto, este fragmento de programa computa a função $F = \{(2k, 2^k) | k \in \mathcal{N}\}$, a qual é uma função parcial de $\mathcal{Z}$ em $\mathcal{Z}$.

5.10.3 Funções não computáveis

As funções não computáveis são aquelas que não podem ser implementadas no computador. Pode-se considerar como funções não computáveis aquelas cujo tempo de execução do programa não é hábil, ou seja, o computador pode levar séculos para implementar tal função.

Exemplo 5.10.4 *Dada uma equação arbitrária da forma $(a+1)^2 + (b+1)^3 = (c+1)^4$, o problema é determinar se a equação é satisfeita por quaisquer números inteiros. Este é o chamado Problema da Equação Diofantina e sabe-se que não existe algoritmo de solução de equações Diofantinas arbitrárias.*

Exemplo 5.10.5 *No exemplo da criptografia do exemplo 5.6.6 os cálculos para a descoberta da chave de decodificação (parâmetros α utilizados para obter $f(\alpha)$)) pode demorar séculos o que pode ser considerado como não computável.*

5.11 Modelos abstratos de um Computador

5.11.1 Máquinas de Estados Finitos

Na maioria dos computadores digitais, existem uma série de circuitos que possibilitam que certas operações sejam realizadas de maneira seqüencial. A seqüência de operações é realizada através de um conjunto de pulsos fornecidos por um 'relógio'. As saídas destes circuitos em um dado instante de tempo são funções das entradas externas e das informações armazenadas no computador no instante considerado. Tais circuitos são chamados de *circuitos seqüenciais*. Um computador pode ser visto como uma rede constituída de um conjunto finito destes circuitos. Cada um destes circuitos pode estar em um único de um conjunto finito de estados a cada instante e portanto podemos considerar um computador como uma rede constituída de um conjunto finito de estados.

Definição 5.11.1 *Uma* máquina seqüencial, *ou* máquina de estados finitos, *é um sistema* $N = \{I, S, O, \delta\lambda\}$, *onde os conjuntos finitos* I, S, *e* O, *são alfabetos que representam respectivamente os símbolos de entrada, estado e saída da máquina.*

Normalmente representamos os alfabetos por

$$I = \{a_0, a_1, ..., a_n\} \;\; S = \{s_0, s_1, ..., s_m\} \;\; O = \{o_0, o_1, ..., s_r\}$$

δ *é uma função, chamada* função de transição de estados *que mapeia* $S \times I \rightarrow S$, *ou seja, em função do estado atual e da entrada, determina qual o próximo estado.* λ *é chamada* função de saída *que mapeia* $S \times I \rightarrow O$, *ou seja, em função do estado atual e da entrada, determina um valor de saída para a máquina. Assumimos também que a máquina inicia em um estado inicial* s_0.

Assim, o modelo abstrato de um computador pode ser dado por um autômata finito. Esta máquina de estados finitos (computador) possui um estado de memória em que dado um comando, tem-se uma resposta. Existe assim uma mudança de estado interno do computador. Esta mudança de memória acarreta a ocorrência de algo no meio exterior. A modelização deste computador pode ser feita através de duas funções. Uma primeira função que diz como atualizar o estado interno do computador (memória do computador) em função do estado anterior e do comando dado (entrada) e uma segunda função que produz a da saída (resposta).

Com o modelo de um computador, tem-se então um conjunto de entradas admissíveis (movimentos do mouse, comandos no teclado), um conjunto de estados internos (posições na memória) e um conjunto de saídas (na tela, impressora tela, etc):

A figura 5.6 a seguir mostra o modelo de uma máquina de estados finitos.

Exemplo 5.11.1 *Um somador seqüencial pode ser definido dentro desta abordagem da seguinte maneira:*

$I = \{00, 01, 10, 11\} \;\; S = \{s_0, s_1\} \;\; O = \{0, 1\}$

$\delta = \{(s_0, 00, s_0), (s_0, 01, s_0), (s_0, 10, s_0), (s_0, 11, s_1),$

$(s_1, 00, s_0), (s_1, 01, s_1), (s_1, 10, s_1), (s_1, 11, s_1)\}$

$\lambda = \{(s_0, 00, 0), (s_0, 01, 1), (s_0, 10, 1), (s_0, 11, 0),$

$(s_1, 00, 1), (s_1, 01, 0), (s_1, 10, 0), (s_1, 11, 0)\}$

o estado inicial é s_0

O diagrama de transição de estados desta máquina de estados finitos pode ser visto na figura 5.7.

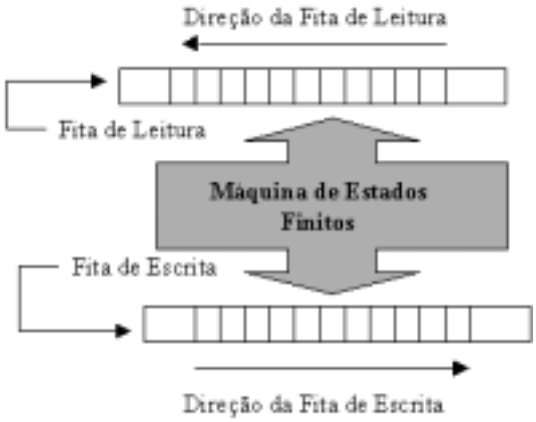

Figura 5.6: Modelo de um Máquina de Estados Finitos

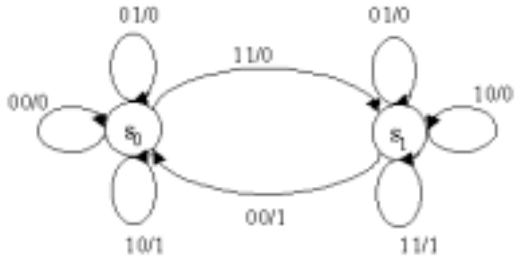

Figura 5.7: Diagrama de Transição de Estados para um somador seqüencial

5.11.2 Máquina de Turing

Em 1936 o matemático britânico Alan Turing imaginou uma máquina abstrata denominada *Turing Machine*. A máquina de Turing é essencialmente um máquina de estados finitos com a habilidade de ler e reler sua entrada e também apagar e escrever sobre a sua entrada, tendo assim uma memória ilimitada. Assim, a máquina de Turing sobrepõe as deficiências de uma máquina de estados finitos [6]. Consistia de uma máquina de estados finitos com uma fita dividida em células, cada célula contendo um símbolo de um alfabeto finito (seqüência de zeros e uns), conforme figura 5.8.

Através de uma cabeça de leitura/escrita a máquina leria uma célula em um dado momento. No próximo instante, dependendo do estado presente na unidade e do símbolo lido, a unidade pára ou completa três ações. Estas ações são: (1) imprime um símbolo do alfabeto na célula lida, (2) vai para o próximo estado e (3)

move a cabeça de leitura da célula para a direita ou para a esquerda.

O conjunto destas ações particulares da Máquina de Turing pode ser descrita por um conjunto de quíntuplas da forma:

$$(x, s, s', x', d)$$

onde:

x é o estado presente

s símbolo lido

s' símbolo impresso

x' novo estado

d direção que a cabeça se move (D para a direita e E para a esquerda).

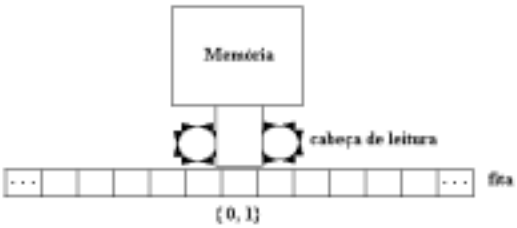

Figura 5.8: Máquina de Turing

Exemplo 5.11.2 *Dada a quíntupla* $(2, 1, 0, 1, D)$. *Se a máquina agir de acordo com as instruções contidas na configuração ilustrada na letra* **a** *moveria para a direita* D *como na configuração da letra* **b** *da figura 5.9.*

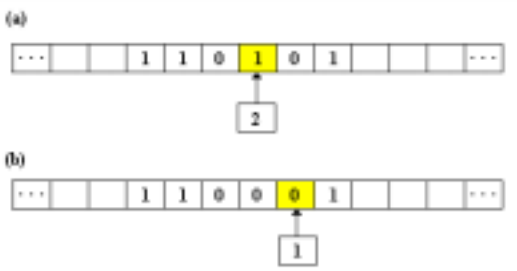

Figura 5.9: Configuração de uma Máquina de Turing

Em termos gerais, uma Máquina de Turing é um dispositivo de entrada e saída, onde a saída só depende da entrada atual (0 ou 1) e da saída anterior. A natureza

da saída não importa. O principal é que as mudanças de estado são definidas por regras de transição. O que Turing provou teoricamente é que pode-se construir uma máquina única, capaz de substituir todas as demais máquinas de Turing. Esta máquina é denominada de *Máquina Universal de Turing*. Esta máquina pode ler instruções, ou seja codificam-se as regras de transição na fita. A cada passo, observa sua própria entrada e as regras de transição para saber o que fazer, ou seja ela é programável. As implicações são que uma única máquina programável pode executar qualquer procedimento lógico bem definido passo a passo. O interessante é que Turing observou este fato cerca de dez anos antes que um verdadeiro computador fosse construído. Maiores informações sobre a Máquina de Turing podem ser obtidas em [6].

Exemplo 5.11.3 *A seguir é mostrado um trecho de um programa em Linguagem C, que quando completo permite a simulação de uma Máquina de Turing.*

```
void RodaMT(statedef tm[], int NumDefs, int itp)
{int state=ESTADOINICIAL;      /* numero do estado atual  */
   char simbolo;               /* ultimo simbolo lido da fita */
   int nadafaz=1;
   long int ciclos=1;
   int PosCabeca;              /* posicao da fita  */
   int proxestado;             /* vai para o proximo estado */
   char EscreveSimb;           /* simbolo a escrever na fita */
   char comando;               /* comando a executar */
   Poscabeca=itp;
   IniciaTela(PosCabeca-20, PosCabeca); /* tracado inicial na tela */
 while (nadafaz) {
  simbolo=LeiaFita(PosCabeca);
  LookUp(tm, NumDefs, estado, simbolo, &proxestado, &EscreveSimb,
  &comando);
  EscreveFita(PosCabeca, EscreveSimb);
  gotoxy(1,20);
  printf("Posicao:%3d  Estado:%-3d  Leitura:%c Proximo Estado:%-3d
  Escrita:%c",PosCabeca, estado, simbolo, proxestado,EscreveSimb);
  printf("Comando:%c  Ciclos:%d", comando ,ciclos);

  switch (comando) {
  case 'D': Movedireita(&PosCabeca, estado);
```

```
          break;
case 'E': Movesquerda(&PosCabeca, estado);
          break;
case 'P': Para();
          nadafaz=0;
          break;
default: printf("\nError: comando ilegal no estado %d leitura &c",
                estado, simbolo);
         exit(1);
    }
estado=proxestado;
ciclos++;   }}
```

Capítulo 6

Estruturas Algébricas

6.1 Introdução

O objetivo dos matemáticos é fazer da matemática uma disciplina disponível a todas as áreas do aprendizado. Esta responsabilidade introduz o conceito de Estrutura Matemática ou Sistema, numa tentativa de estabelecer uma forma na qual procura se encontrar analogias que se apliquem a outras áreas da Matemática bem como ao Universo físico.

A idéia de Estrutura ou Sistema Algébrico inicia pela aceitação inicial de várias noções sobre uma base intuitiva. A estrutura em si mesma é um conjunto de elementos abstratos, termos não definidos, e várias regras. O que se verifica é qu,e diferentes sistemas vão possuir diversas propriedades em comum. Esta observação fornece a motivação para o estudo de sistema algébricos abstratos em que certas propriedades podem ser tomadas como axiomas do sistema. Assim, resultados que são vãlidos para o sistema abstrato, permanecem válidas para todos os sistemas algébricos nos quais os axiomas sejam verdadeiros.

Ao longo deste capítulo serão introduzidos vários conceitos importantes sobre os Sistemas Algébricos. O conceito de *isomorfismo*, por exemplo, estabelece que dois sistemas algébricos que são isomórficos entre si, são estruturalmente indistingüíveis e, portanto, os resultados de operações em um sistema podem ser obtidos através de operações no outro sistema, simplesmente renomeando o nomes dos elementos e das operações.

Veremos também as diferentes estruturas algébricas, suas propriedade e suas aplicações em diferentes áreas da Ciência da Computação.

Semigrupos são umas das estruturas algébricas mais simples e que satisfazem as propriedades de fechamento e associatividade. Eles são muito importantes na teoria

de máquinas seqënciais, linguagens formais e em certas aplicações relacionadas à aritmética computacional, como, por exemplo, a multiplicação.

Um monóide, além de ser um semigrupo, também satisfaz a propriedade de possuir um elemento identidade. Os monóides são utilizados em várias aplicações, especialmente na área de análise sintática e linguagens formais.

Grupos, por sua vez, são monóides que também possuem a prorpiedade de possuirem um elemento inverso. A aplicação da teoria de grupos é importante no projeto de somadores rápidos e códigos com capacidade de correção de erros.

6.2 Conceitos de Estruturas Algébricas

Toda estrutura algébrica tem seu ponto de origem em vários termos não definidos, tais como: conjunto, número e ponto. Conceitos são definidos sobre a base de outros conceitos e termos.

Para o propósito deste trabalho, chamaremos de um *Sistema Algébrico*, ou simplesmente uma *Álgebra* a um sistema constituído de um conjunto e uma ou mais operações binárias sobre este conjunto. Alguns autores, além de operações sobre o conjunto, incluem relações entre os elementos do conjunto, no que então passa a ser conhecido como *Estrutura Algébrica*.

Uma operação binária será denotada por meio de um símbolo, tal como: $*$, $\triangle$, $+$, $\oplus$, etc. e o resultado da operação binária sobre os elementos, $x_1, x_2 \in X$, é expresso escrevendo-se $x_1 * x_2$. Para um conjunto X finito, pode também ser conveniente representar a operação binária através de uma tabela.

Também denotaremos um Sistema Algébrico por $(X, f_1, f_2, ...)$ onde X é um conjunto não vazio e $f_1, f_2, ...$ são operações em X.

A seguir veremos alguns exemplos de Sistemas Algébricos e examinaremos suas propriedades. Por "propriedade de um sistema algébrico" ou axioma, entendemos uma propriedade exibida pelas suas operações.

Exemplo 6.2.1 *Seja $\mathcal{I}$ o conjunto dos inteiros. Considere o sistema algébrico $(\mathcal{I}, +, \times)$ onde $+$ e $\times$ são as operações de adição e multiplicação em $\mathcal{I}$. Uma lista de importantes propriedades destas operações será exibida a seguir. As propriedades associadas com as operações de adição e multiplicação serão rotuladas com as letras* **A** *e* **M** *respectivamente. Estas propriedades ou axiomas serão constantemente citadas quando examinarmos outros sistemas algébricos.*

(A-1) Associatividade - *Para quaisquer= $a, b, c \in \mathcal{I}$*

$$(a + b) + c = a + (b + c)$$

(A-2) Comutatividade - *Para quaisquer* $a, b \in \mathcal{I}$

$$a + b = b + a$$

(A-3) Elemento Identidade ou Neutro - *Existe um elemento* $0 \in \mathcal{I}$ *tal que para todo* $a \in \mathcal{I}$

$$a + 0 = 0 + a = a$$

Aqui 0 *é o elemento neutro com relação à adição.*

(A-4) Elemento Inverso - *Para cada* $a \in \mathcal{I}$*, existe um elemento em* $\mathcal{I}$ *denotado por* $-a$ *e chamado o* negativo de a *tal que*

$$a + (-a) = 0$$

(M-1) Associatividade - *Para quaisquer* $a, b, c \in \mathcal{I}$

$$(a \times b) \times c = a \times (b \times c)$$

(M-2) Comutatividade - *Para quaisquer* $a, b \in \mathcal{I}$

$$a \times b = b \times a$$

(M-3) Elemento Identidade ou Neutro - *Existe um elemento* $1 \in \mathcal{I}$ *tal que para todo* $a \in \mathcal{I}$

$$a \times 1 = 1 \times a = a$$

Aqui 1 *é o elemento neutro com relação à multiplicação.*

(D) Distributividade - *Para quaisquer* $a, b, c \in \mathcal{I}$

$$a \times (b + c) = (a \times b) + (a \times c)$$

(C) Cancelamento - *Para* $a, b, c \in \mathcal{I}$ *e* $a neq 0$

$$a \times b = a \times c \rightarrow b = c$$

A seguir veremos outros exemplos de sistemas algébricos com duas operações binárias e que compartilham da maior parte das propriedades de $(\mathcal{I}, +, \times)$ listadas no exemplo anterior.

Exemplo 6.2.2 *Seja* $\Re$ *o conjunto dos números reais e* $+$ *e* $\times$ *as operações de adição e multiplicação em* $\Re$*. O sistema algébrico* $(\Re, +, \times)$ *satisfaz todas as propriedades dadas pelo sistema* $(\mathcal{I}, +, \times)$*. Existem ainda certas propriedades que distinguem os dois sistemas, estas propriedades serão vistas adiante.*

Exemplo 6.2.3 *No sistema algébrico* $(\mathcal{N}, +, \times)$ *onde* $\mathcal{N}$ *é o conjunto dos números naturais e as operações* $+$ *e* $\times$ *são de adição e multiplicação, são satisfeitas todas as propriedades listadas para* $(\mathcal{I}, +, \times)$*, com exceção de* **(A-4)**.

Exemplo 6.2.4 *Seja* U *um conjunto Universo e* $\rho(U)$ *seu conjunto potência. Se denotarmos as operações de união e interseção em* $\rho(U)$ *por* $+$ *e* $\times$ *respectivamente, então teremos o sistema algébrico* $(\rho(U), +, \times)$ *com* $\emptyset$ *e* U *como os elementos distintos equivalentes de* 0 *e* 1*, e este sistema satisfaz todas as propriedades listadas, exceto* **(A-4)** *e* **(C)**.

Exercício 6.2.1 *Seja* $\Re$ *o conjunto dos números reais e o sistema* $(\Re, *)$ *onde* $*$ *define a operação de média entre 2 elementos de* $\Re$*, isto é,* $a * b = (a + b)2$*, onde* a *e* $b \in \Re$*. Possue esta operação as propriedades de fechamento, comutatividade e associatividade?*

- *Fechamento:* $\Re$ *é fechado com respeito da operação* $*$*, uma vez que a média de dois números reais também é um número real.*

- *Comutatividadde:*

$$a * b = \frac{a+b}{2} \quad e \quad b * a = \frac{b+a}{2} = \frac{a+b}{2}$$

  Logo o sistema é comutativo com respeito à operação $*$.

- *Associatividade:*

$$(a * b) * c = \frac{\frac{a+b}{2} + c}{2} \quad e \quad a * (b * c) = \frac{a + \frac{b+c}{2}}{2}$$

$$(a * b) * c \neq a * (b * c)$$

  Logo o sistema não é associativo com respeito à operação de $*$.

Exercício 6.2.2 *Seja a operação* $*$ *definida sobre o conjunto* $U = \{e, o\}$ *e descrita pela tabela 6.1. Possue esta operação as propriedades de fechamento, comutatividade e associatividade?*

Desde que todos os resultados obtidos da operação $*$ *são elementos de* U*, pode-se dizer que* $*$ *é fechado em* U*. Além disso, a operação* $*$ *é comutativa, uma vez que um estudo da tabela mostra uma simetria com relação à diagonal principal.*

Verificando se é associativa:

$$(e * o) * o = e * (o * o)$$

$*$	e	o
e	e	o
o	o	e

Tabela 6.1: Tabela para operação $*$ sobre o conjunto $\{e, o\}$

$$(e * e) * o = e * (e * o)$$

$$(o * o) * e = o * (o * e)$$

Conclui-se que $*$ é associativa.

Resumindo, um sistema algébrico consiste de um conjunto de elementos, operações, postulados, teoremas e definições. Se A representa um conjunto de elementos e $*$ uma operação, logo $A : *$ simbolizará um sistema algébrico. O conjunto de elementos é caracterizado ou desrito inicialmente por meio de um conjunto de postulados que representam as regras ou leis do sistema e governam o significado dos símbolos utilizados para representar os elementos e operações do sistema. Os teoremas são formados e provados como uma conseqüência de um conjunto de postulados e regras logicas. Quando estes teoremas são provados, possuem a mesma validade no sistema como a do conjunto original de postulados, uma vez que estes teoremas são uma conseqüência lógica dos postulados.

A partir desses axiomas outras regras podem ser demonstradas. Por exemplo, aplicando-se rigorosamente os axiomas e presumindo-se nada mais, nós podemos provar rigirosamente a regra aparentemente óbvia de que

$$\text{se } m + k = n + k, \text{ então } m = n.$$

Para começar podemos declarar que

$$m + k = n + k.$$

Então, pelo axioma **(A-4)**, façamos l ser um número tal que $k + l = 0$, assim

$$(m + k) + l = (n + k) + l.$$

Então, pelo axioma **(A-1)**,

$$m + (k + l) = n + (k + l).$$

Tendo-se em mente que $k + l = 0$, nós sabemos que

$$m + 0 = n + 0.$$

E aplicando o axioma **(A-3)** nós podemos finalmente declarar o que nos propusemos a demonstrar:

$$m = n.$$

É possível construir diferentes sistemas algébricos dependendo da escolha de diferentes conjuntos de elementos, operações e postulados. Um sistema particular não necessariamente melhor que o outro; cada um é estudado na base dos seus próprios méritos e interpretações. depois que um sistema algébrico particular foi construído, ele pode ser interpretado de diferentes maneiras. Se todos os postulados do sistema são verdadeiros para uma interpretação específica dos termos e símbolos, então esta interpretação específica representa um "modelo". A ciência aplicada estuda um sistema abstrato particular de modo a enquadrá-lo com algum aspecto do universo físico. Algumas vezes ela tem sucesso, outras ela erra, não porque o sistema algébrico seja incorreto, mas sim porque a situação física não é um modelo ou uma interpretação correto do sistema considerado.

Exemplo 6.2.5 *Seja S um conjunto não vazio e $P(S)$ seu conjunto potência. Para quaisquer conjuntos A e $B \in P(S)$, podemos definir as operações $+$ e $\times$ em $P(S)$ como:*

$$A + B = (A - B) \cup (B - A) = (A \cap B) \cup (B \cap A)$$
$$A \times B = A \cap B \ (\times \text{ não é o produto cartesiano})$$

O sistema algébrico $(P(S), +, \times)$ satisfaz todas as proriedades listadas, com exceção de **(C)**.

Exercício 6.2.3

- *Quais seriam os elementos identidade para as operações de $+$ e $\times$ respectivamente?*
- *Mostre que A é o inverso de A com relação à operação de $+$ para qualquer $A \in P(S)$.*

Exemplo 6.2.6 *Considere o conjunto $B = \{0, 1\}$ e as operações $+$ e $\times$ em B dadas pelas tabelas a seguir*

O sistema algébrico $(B, +, \times)$ satisfaz todas as propriedades listadas anteriormente.

$+$	0	1
0	0	1
1	1	0

Tabela 6.2: Tabela da operação $+$

$\times$	0	1
0	0	0
1	0	1

Tabela 6.3: Tabela da operação $\times$

Através destes exemplos podemos claramente perceber que um grande número de sistemas algébricos possuem várias propriedades em comum àquelas apresentadas pelo sistema $(I, +, \times)$.

Ao invés de estudar cada um destes sistemas individualmente, seria interessante listar uma série de propriedades e tirar conclusções sobre qualquer sistema que apresente as mesmas propriedades. As propriedades consideradas são encaradas como axiomas, e qualquer conclusão válida obtida através dos axiomas para um determinado sistema algébrico, será válida para todos os outros sistemas algébricos para os quais os axiomas também se aplicam.

6.3 Estruturas com uma operação interna

Os sistemas algébricos vistos nos exemplos anteriores continham duas operações binárias que eram denotadas por $+$ e $\times$. Estes sistemas algébricos não são os mais simples. Nesta seção veremos exemplos e definições de sistemas algébricos constituídos apenas de uma operação binária.

Definição 6.3.1 Magma *é a estrutura algébrica mais simples. Considera-se um conjunto dotado de apena um única operação interna. Denota-se por S ao conjunto e por $\circ$ a operação.*

$$(S, \circ)$$

Definição 6.3.2 *Seja S um conjunto não-vazio e $\circ$ uma operação binária em S. O sistema algébrico $(S.\circ)$ é chamado um* semigrupo *se a operação $\circ$ for associativa.*

Ou seja, $(S, \circ)$ *é um semigrupo se para todo* $x, y, z \in S$,

$$(x \circ y) \circ z = x \circ (y \circ z)$$

Definição 6.3.3 *Um semigrupo* $(M, \circ)$ *com um elemento identidade com relação à operação* $\circ$ *é chamado um* monóide. *Ou seja, um sistema algébrico* $(M, \circ)$ *é chamado monóide se para todo* $x, y, z \in S$

$$(x \circ y) \circ z = x \circ (y \circ z)$$

e existir um elemento $e \in M$ *tal que para todo* $x \in M$,

$$e \circ x = x \circ e = x$$

Exemplo 6.3.1 *Seja* $\mathcal{N}$ *o conjunto dos números naturais. Então* $(\mathcal{N}, +)$ *e* $(\mathcal{N}, \times)$ *são monóides com elementos identidade 0 e 1 respectivamente.*

Exemplo 6.3.2 *Seja* $\mathcal{E}$ *o conjunto dos números pares positivos excluindo o zero. Então* $(\mathcal{E}, +)$ *e* $(\mathcal{E}, \times)$ *são semigrupos, mas não são monóides.*

Exemplo 6.3.3 *Seja* $\mathcal{I}$ *o conjunto dos números ímpares positivos. Então* $(\mathcal{I}, +)$ *não é um sistema algébrico (porque não é fechado), enquanto* $(\mathcal{I}, \times)$ *é um monóide.*

Definição 6.3.4 *Se em um semigrupo ou monóide* $(S, \circ)$, *a operação* $\circ$ *é comutativa, então o semigrupo ou monóide são chamados* comutativos.

Exemplo 6.3.4 *Seja* $\mathcal{N}$ *o conjunto dos números naturais. Então* $(\mathcal{N}, +)$ *é um monóide comutativo.*

Exemplo 6.3.5 *Seja* $A = \{a, b, c, ..., z\}$ *o conjunto das letras do alfabeto, seja* S *o conjunto de palavras formadas pelas letras do alfabeto e seja* $\circ$ *a operação de concatenação de palavras de* S. *Então o sistema algébrico* $(S, \circ)$ *é um semigrupo. Se admitirmos um palavra vazia* Λ, *então* $(S, \circ)$ *é um monóide. No entanto,* $(S, \circ)$ *não é comutativo pois*
ata $\circ$ *bola neq bola* $\circ$ *ata.*

Definição 6.3.5 *Um* grupo $(G, \circ)$ *é um sistema algébrico na qual a operação* $\circ$ *satisfaz três condições:*

1. *Para todo* $x, y, z \in G$,

$$(x \circ y) \circ z = x \circ (y \circ z)$$

2. *Existir um elemento* $e \in M$ *tal que para todo* $x \in G$,

$$e \circ x = x \circ e = x$$

3. *Para todo* $x \in G$, *existe um elemento denotado por* $x^{-1} \in G$ *tal que*

$$x \circ x^{-1} = x^{-1} \circ x = e$$

A existência de um elemento inverso para todo elemento de G garante a existência de solução para toda a equação do tipo $a \circ x = b$, onde $a, b \in G$. A solução é dada por $x = a^{-1} \circ b$. Do mesmo modo, a existência do inverso de cada elemento implica que a propriedade de cancelamento é válida, isto é:

$$a \circ b = a \circ c \; rightarrow b = c$$

$$b \circ a = c \circ a \; rightarrow b = c$$

para todo $a, b, cinG$.

Definição 6.3.6 *O número de elementos de* G, *quando* G *é finito, é denotado por* $|G|$ *e é chamado de* ordem do grupo $(G, \circ)$.

Definição 6.3.7 *Um grupo* $(G, \circ)$ *no qual a operação* $\circ$ *é comutativa é chamado um* Grupo Abeliano.

Exemplo 6.3.6 *Seja* $\mathcal{Z}$ *o conjunto dos inteiros. A álgebra* $(\mathcal{Z}), +)$ *é um grupo abeliano.*

Exemplo 6.3.7 *O conjunto* $\mathcal{Q}$ *dos números racionais excluindo o zero é um grupo abeliano sobre a operação de multiplicação.*

6.4 Estruturas com duas operações internas

Os sistemas algébricos com uma operação interna estudados até agora, não são adequados para descrever o sistema dos números reais, pois este sistema envolve duas operações básicas, a adição e a multiplicação. Devemos então considerar um sistema

algébrico abstrato chamado *ANEL*, que é um caso especial de um grupo no qual definimos uma operação adicional, capaz de satisfazer certas propriedades. Outros sistemas algébricos, com duas operações internas podem ser obtidos, adicionando-se restrições aos anéis.

Definição 6.4.1 *Um sistema algébrico* $(S, +, \cdot)$ *é chamado um* anel *se as operações binárias* $+$ *e* $\cdot$ *em* S *satisfazem as três propriedades a seguir:*

1. $(S, +)$ *é um grupo abeliano.*
2. $(S, \cdot)$ *é um semigrupo.*
3. *A operação* $\cdot$ *é distributiva com respeito à* $+$*, isto é, para todo* $a, b, c \in S$*,*

$$a \cdot (b + c) = a \cdot b + a \cdot c$$

e

$$(b + c) \cdot = b \cdot a + c \cdot a$$

Exemplos conhecidos de anéis são os conjuntos dos números inteiros, números reais, números racionais, números pares e números complexos, sobre as operações de adição e multiplicação. Devido a nossa familiaridade com estes exemplos, e comum nos referirmos à operação $+$ como adição e à operação $\cdot$ como multiplicação em um anel $(S, +, \cdot)$, embora estas operações não sejam necessariamente adições e multiplicações como as conhecemos. Por convenção, é comum também chamarmos o elemento identidade de $(S, +)$ como *identidade aditiva* e denotá-lo por 0. Do mesmo modo, se $(S, \cdot)$ é um monóide, então o elemento identidade com relação à $\cdot$ é chamado de *identidade multiplicativa* e é denotado por 1. Também o *inverso aditivo* de um elemento a é denotado por $-a$, enquanto o *inverso multiplicativo*, se existir, é denotado por a^{-1}.

Dependendo das propriedades do sistema $(S, \cdot)$, vários casos especiais de anéis podem ser definidos.

Definição 6.4.2 *Se* $(S, \cdot)$ *for um monóide, então* $(S, +, \cdot)$ *é chamado de* anel unitário.

Definição 6.4.3 *Se* $(S, \cdot)$ *comutativo, então* $(S, +, \cdot)$ *é chamado de* anel comutativo.

Aprofundando nossa observação, não pdemos esperar que $(S, \cdot)$ seja um grupo, uma vez que um grupo com mais de um elemento não pode possuir um elemento zero. Senão vejamos:

Suponhamos que S seja um grupo e que $0 \in S$. Então

$$0 \cdot 1 = 1 \cdot 0 = 0$$

o que satisfaz a segunda condição e portanto $e = 1$. Mas

$$0 \cdot 0^{-1} \neq 1$$

o que contradiz a terceira condição, qual seja

$$x \cdot x^{-1} = x^{-1} \cdot x = e$$

Devemos então perguntar primeiramente se $(S - \{0\}, \cdot)$ é fechado com relação à operação $\cdot$. Se ele for fechado, então teremos para todo $a, b \in S$ tal que $a \neq 0$ e $b \neq 0$, $a \cdot b \neq 0$, e chamamos $(S, +, \cdot)$ um anel *sem divisores de zero*.

$$a \cdot b = 0 \rightarrow a = 0 \vee b = 0$$

Definição 6.4.4 *Um anel comutativo $(S, +, \cdot)$ com elemento identidade e sem divisores de zero é chamado um* domínio de identidade.

Assumimos na definição de *domínio de identidade* que o anel $(S, +, \cdot)$ possui mais de um elemento; isto é, que ele possui ao menos um elemento diferente de zero.

Nosso próximo questionamento se refere a descobrir se $(S - \{0\}, \cdot)$ é um grupo. Este questionamento caonduz a seguinte definição:

Definição 6.4.5 *Um anel comutativo $(S, +, \cdot)$ que possui mais de um elemento tal que todo elemento diferente de zero possua um inverso multiplicativo em S é chamado um* campo.

O anel dos inteiros é um exemplo de um domínio de identidade que *NÃO* é um *campo*. Os anéis dos números reais e racionais são exemplos de campos.

Exemplo 6.4.1 *O sistema algébrico $(\mathcal{Z}_n, +, \cdot_n)$ consistindo das classes de equivalência geradas pela relação* módulo congruente n *(o resto da divisão dos elementos de $\mathcal{Z}$ por n), para um dado n do conjunto dos inteiros é um anel. As operações $+_n$ e $\cdot_n$ são definidas como:*

Para quaisquer $[i]$, e $[j] \in \mathcal{Z}$

$$[i] +_n [j] = [(i + j)\ (mod\ n)]$$

$$[i] \cdot_n [j] = [(i \cdot j)\ (mod\ n)]$$

Observe que para $n = 6$, $(\mathcal{Z}_6, +_6, \cdot_6)$ não é um domínio de identidade, pois $[3] \cdot [2] = [0]$. Por outro lado, $(\mathcal{Z}_7, +_7, \cdot_7)$ é um domíinio de identidade. De fato, $(\mathcal{Z}_n, +_n, \cdot_n)$ é um campo se e somente se n é primo.

Referências Bibliográficas

[1] E. Alencar Filho. *Teoria Elementar dos Conjuntos.* Nobel, São Paulo, 21ª edição, 1990.

[2] Jorge M. Barreto and José Augusto Mariz de Mendonça. Estudo da conversão análogo digital. Relatório técnico, Descrição de parte do projeto apresentado pelo término do curso de Engenheiro Eletrônico, Instituto Militar de Engenharia, Rio de Janeiro, 1960.

[3] Louis Couffignal. *Sur l'analyse mécanique: application aux machines à calcular et aux calculs de la mécanique céleste.* Springer-Verlag, Berlin, 1975.

[4] N. C. Davis and S. E. Goodman. The soviet bloc's unified system of computers. *Computing surveys*, junho 1978.

[5] P.A. et al Fejer. *Mathematical Foundations of Computer Science.* Spring-Verlag, New York, 1990.

[6] J.L. Gersting. *Mathematical Structures for Computer Cience.* Computer Science Press, New York, 3ª edição, 1993.

[7] C.A. et al. Guelli. *Conjuntos, Relações, Funções, Inequações.* Editora Moderna, São Paulo, 1979.

[8] P. Halmos. *Teoria Intuitiva de Los Conjuntos.* Compañia Editorial Continental S.A., México, 4ª edição, set. 1967.

[9] S. Lipschutz. *Teoria Elementar dos Conjuntos.* Coleção Schaum. McGraw-Hill do Brasil, São Paulo, 1990.

[10] P. Papy. *Mathématique Moderne.* Marcel Didier, Bruxelles, 4ª edição, 1968.

[11] B. Randell. *The Origins of Digital Computers: selected papers.* Springer-Verlag, Berlin, 1975.

[12] P. Suppes. *Axiomatic Set Theory*. Dover Publications, New York, 1972.